

Rational authentication protocols

Long Nguyen
Oxford University Computing Laboratory

A rational intruder

Powerful & wants to maximise payoff.

Does no worse by attacking all the time.

In each protocol run:

- Probability ε : success & payoff U^+
- Probability $1 - \varepsilon$: failure & payoff U^- for denial of service & further knowledge of password

We want to discourage this type of intruder.

Protocol transformation

Probability α , a honest node A pursues irrational behaviours: authenticate useless data.

Waste of time for the other honest node B .

Intruder is given payoff U for this behaviour of A .

Summary of payoffs

Strategy of intruder	Strategy of party A	Outcome of protocol	Payoff of intruder
Does not attack	Faithful	Succeed	0
	Unfaithful <small>$U^+ + \epsilon$</small>	Succeed	U
Attack	Any	Succeed	U^+
		Fail	U^-

$$U^+ > U > U^-$$

Summary of payoffs

Strategy of intruder	Strategy of party <i>A</i>	Outcome of protocol	Payoff of intruder
Does not attack	Faithful	Succeed	0
	Unfaithful		U
Attack	Faithful	Succeed	U^+
	Unfaithful		$< U^+$
	Faithful	Fail	U^-
	Unfaithful		$< U^-$

Single-run attack

If intruder does not attack, expected payoff: αU

If intruder attacks, expected payoff: $\varepsilon U^+ + (1-\varepsilon)U^-$

To discourage the intruder, we must have

$$\alpha U > \varepsilon U^+ + (1-\varepsilon)U^-$$

$$\alpha > \varepsilon U^+/U + (1-\varepsilon)U^-/U = U^-/U + \varepsilon(U^+ - U^-)/U$$

ε can be made arbitrarily small relative to U^+ .

Multiple-run attack

An intruder can attack up to k protocol runs

If an intruder attacks, it quits iff

- Succeeds in the t^{th} attempt, where $t \leq k$, or
- Fails in all k attempts.

We want to discourage this kind of intruder.

Password-based protocol

Password is chosen from $\{1, \dots, n\}$

- First guess is correct with $\varepsilon = \varepsilon_1 = 1/n$
- Second guess is correct with $\varepsilon_2 = 1/(n-1)$
- t^{th} guess is correct with $\varepsilon_t = 1/(n-t+1)$

At most n guesses: $k \leq n$

Game of a k -run attack

No. of attempt	Outcome	Probability	Payoff of intruder
1	Succeed	$\varepsilon = \varepsilon_1 = 1/n$	U^+
2	Succeed	$(1-\varepsilon_1)\varepsilon_2 = 1/n$	$U^- + U^+$
3	Succeed	$(1-\varepsilon_1)(1-\varepsilon_2)\varepsilon_3 = 1/n$	$2U^- + U^+$
....
t	Succeed	$(1-\varepsilon_1)\cdots(1-\varepsilon_{t-1})\varepsilon_t = 1/n$	$(t-1)U^- + U^+$
....
k	Succeed	$(1-\varepsilon_1)\cdots(1-\varepsilon_{k-1})\varepsilon_k = 1/n$	$(k-1)U^- + U^+$
k	Fail	$(1-\varepsilon_1)\cdots(1-\varepsilon_k) = (n-k)/n$	kU^-

Attacking up to k runs

The expected (or average) number of attempts:

$$N = 1/n + 2/n + \dots + k/n + k(n-k)/n = \frac{k(2n - k + 1)}{2n}$$

The expected payoff of the intruder:

$$\begin{aligned} P &= U^+/n + (U^- + U^+)/n + \dots + ((k-1)U^- + U^+)/n + kU^-/n \\ &= kU^+/n + k(2n-k-1)U^-/(2n) \end{aligned}$$

Attacking up to k runs

If intruder does not attack, expected payoff: αUN

To discourage this intruder, we must have

$$\alpha UN > P$$

$$\alpha > [\varepsilon U^+/U + (1-\varepsilon)U^-/U] + \Delta(U^+ - U^-)/U$$

where $\Delta = \frac{k-1}{n(2n-k+1)}$

Other related work

Rational manual authentication protocol.

Authentication protocol based on a challenge-response (or distance-bounding) exchange

Paper: <http://eprint.iacr.org/2011/070>

Or my website.

Password-based protocol

1. $A \rightarrow B : A \parallel E_{pw}(g^x)$

2. $B \rightarrow A : E_{pw}(g^y) \parallel \text{hash}(sk \parallel 1)$

where $sk = \text{hash}(A \parallel B \parallel g^x \parallel g^y \parallel g^{xy})$

3. $A \rightarrow B : \text{hash}(sk \parallel 2)$

Password “pw” is taken from $\{1, \dots, n\}$

Summary of payoffs

Strategy intruder	Strategy of A	Strategy of B	Protocol outcome	Payoff of intruder
Does not attack	Faithful	Faithful	Succeed	0
	Unfaithful			U_1
	Faithful	Unfaithful		U_1
	Unfaithful			U_2
Attack	Faithful	Faithful	Succeed or Fail	U^+_1 or U^-_1
	Unfaithful			U^+_2 or U^-_2
	Faithful	Unfaithful		U^+_2 or U^-_2
	Unfaithful			U^+_3 or U^-_3

Strategy of intruder	Strategy of all parties	Protocol outcome	Payoff of intruder
Does not attack	All faithful	Succeed	0
	At least 1 faithful & 1 unfaithful		U_1
	All unfaithful		U_2
Attack	At least 1 faithful	Succeed or Fail	U^+_1 or U^-_1
	Unfaithful		U^+_2 or U^-_2

Authentication protocols

Honest nodes always incorporate to agree on the same data.

Honest nodes are not self-interested.

But the intruder is self-interested and rational.

Manual authentication protocol

1. $A \rightarrow B : m_A \parallel c_A$

2. $B \rightarrow A : m_B \parallel c_B$

where $c_x \parallel d_x = \text{commit}(m_x, R_x)$

3. $A \rightarrow B : d_A$

4. $B \rightarrow A : d_B$

5. $A \rightarrow B : R_A \text{ XOR } R_B$

Manual authentication protocol

The chance of a successful one-shot attack remains unchanged regardless of how many times an attack is launched.

We denote ϵ the chance of a successful attack on a single protocol run.

Game in a k -run attack

No. of attempt	Outcome	Probability	Payoff of intruder
1	Succeed	ε	U^+
2	Succeed	$(1 - \varepsilon) \varepsilon$	$U^- + U^+$
3	Succeed	$(1 - \varepsilon)(1 - \varepsilon)\varepsilon$	$2U^- + U^+$
....
t	Succeed	$(1 - \varepsilon)^{t-1} \varepsilon$	$(t-1)U^- + U^+$
....
k	Succeed	$(1 - \varepsilon)^{k-1} \varepsilon$	$(k-1)U^- + U^+$
k	Fail	$(1 - \varepsilon)^k$	kU^-

Multiple-run attacks

It does not matter how many runs an intruder attacks a protocol, to discourage the intruder:

$$\alpha > \varepsilon U^+ / U + (1 - \varepsilon) U^- / U$$