Key Levels and Securing Key Predistribution Against Node Captures

Jacek Cichoń, Jarosław Grząślewicz, Mirek Kutyłowski

Wrocław University of Technology,

ACNS 2009

Application Scenario

simple devices, symmetric methods, ad hoc connections

Network

- a network of simple devices, equipped with symmetric algorithms only
- unpredictable which devices will communicate
- all devices from the same provider

Application Scenario

simple devices, symmetric methods, ad hoc connections

Network

- a network of simple devices, equipped with symmetric algorithms only
- unpredictable which devices will communicate
- all devices from the same provider

Requirement

- no plaintext transmission
- two devices establish a session key when they meet

Random Key Predistribution

simple devices, symmetric methods

Initialization

- The system provider keeps a secret pool $\mathcal{K}$ of keys selected at random.
- Before being used a device receives k keys from $\mathcal{K}$ chosen at random.

Initialization

- The system provider keeps a secret pool $\mathcal{K}$ of keys selected at random.
- Before being used a device receives k keys from $\mathcal{K}$ chosen at random.

Setting up a connection between A and B

- A and B determine the keys they share, say $k_{i_1}, \ldots, k_{i_t}$,
- A and B compute the session key

$$\mathcal{K} = F(k_{i_1}, \ldots, k_{i_t}, A, B, ...)$$

based on the birthday paradox

Attack
node captures

Collecting keys

An adversary

1. gets devices
2. retrieves the keys contained inside (may be in a destructive way)

Scale of the problem

- no physical protection of the devices
- cheap devices are not tamper proof

Goal

Improve the situation!

- many diverse proposals in the literature,
- **we provide an additional security mechanism for almost all predstribution techniques**

Key Levels Technique

T Levels Scheme

1. each single key k from the basic method corresponds to an set of keys

$$K_1, K_2, \ldots, K_T$$

2. the keys related in a one-way fashion:

$$K_1 = K \quad \text{and} \quad K_{i+1} = G(K_i) \quad \text{for } i = 1, \ldots, T-1$$

where G is easy to compute but infeasible to invert

Establishing a Connection

T level scheme

Mechanism

if A holds K_i and B holds K_j, then $K_{\max(i,j)}$ used for establishing the shared key

computing K_s from K_t, for $s > t$, is easy,

it is infeasible for $s < t$

Gain

if an adversary holds

$$K_t \quad \text{for } t > \max(i,j),$$

then the connection between A and B is secure

(with A, B and the adversary holding (a version of) K)

Problems

How to assign the levels

1. the uniform distribution is not optimal
2. example: the optimal pbb of choosing K_1, K_2, K_3, K_4:

$$0.437055, \quad 0.218527, \quad 0.182106, \quad 0.162312$$

3. we show an effective procedure to find the optimal probabilities

Problems

How to assign the levels

1. the uniform distribution is not optimal
2. example: the optimal pbb of choosing K_1, K_2, K_3, K_4:
   $$0.437055, \quad 0.218527, \quad 0.182106, \quad 0.162312$$
3. we show an effective procedure to find the optimal probabilities

Probability of adversary's failure

assumption: A, B and the adversary use a version of K

1. for 2 levels it is $\frac{4}{27}$, pbb increases with the number of levels
2. for infinite number of levels:
   - it reaches $\frac{1}{3}$
   - no matter what probability density is used

Attack Cost

the expected number of devices corrupted until a connection becomes insecure

Theorem (2 level case, p is the probability to choose level 1)

Let $L_{m,p}$ denote the number of steps after which adversary collects all keys for compromising connection based on m shared keys. Then

$$E[L_{m,p}] = \int_0^\infty \left(1 - \frac{H(t)}{e^t}\right) dt \,, \tag{1}$$

where $H(z) = \left(e^{z/m} - 1 - p^2(e^{qz/m} - 1)\right)^m$ and $q = 1 - p$.

Attack Cost

the expected number of devices corrupted until a connection becomes insecure

Corollary

- For $m = 1$ the optimal value of p is 0.5; then $E[L_m] \approx 1.25$.
- If $m = 10$, then the optimal value of p is 0.32164; in this case we get $E[L_m] = 40.9724$, so $E[L_m] = 1.39887 \cdot m \cdot H_m$, where $H_m =$ the mth harmonic number. So the actual cost of breaking the transmission is increased by $\approx 40\%$

Very large number of levels

From factor 1 improve to 1.5 as a limit value.

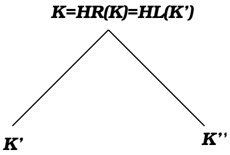
Trees

an extension with no *weak keys*

Idea

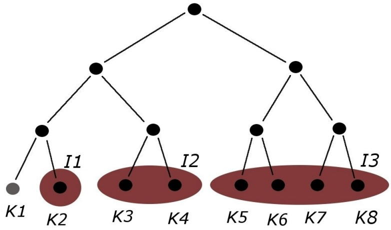
Instead of a single key K or a chain of keys $K_0, K_1 \ldots$, we can construct the following tree $T_{\hat{K}}$ of keys:

- each node of the tree is labeled with a key, the root is labeled with $\hat{K}$,
- if a node is labeled with key K, then its parent is labeled with $H_i(K)$, where $i = L, R$



Trees

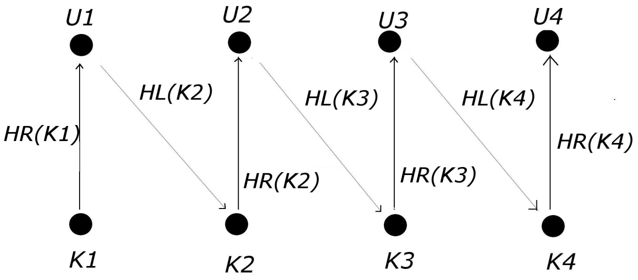
an extension with no *weak keys*



a tree containing keys $K_1, \ldots K_8$, if adversary is holding the key K_1, then the communication between A and B is not broken if they both hold keys from $I1 = \{K_2\}$ or from $I2 = \{K_3, K_4\}$ or from $I3 = \{K_5, K_6, K_7, K_8\}$

Reducing the number of keys in a device

keeping connectivity



1. special choice of keys in the pool
2. the devices do not have to share a key, subsequent keys can be used as well

Conclusions

Further constructions and details

to be presented during ALGOSENSORS'2009

Main features

attack resilience improved moderately, but practically with no cost