Observations on Linear Key Predistribution Schemes and Their Applications to Group Deployment of Nodes

Alexey Urivskiy

JSC "InfoTeCS"
ourivski@mail.ru, urivskiy@infotecs.ru

June 20, 2012

Key Predistribution

Goal: reduce the number of keys during generation, transmission and storing.

Method: Key Predistribution Schemes — KPS.

- a network of N nodes;
- a trusted authority;
- a set of secret keys $\mathcal{K}$ — the key pool;
- a set of node's keys $\mathcal{S}_j \subset \mathcal{K}$ — the key block of the node;
  - (usually) not being changed during network operation;;
- the pairwise (common) key $\kappa_{j_1 j_2} = KDF(\mathcal{S}_{j_1}, j_2) = KDF(\mathcal{S}_{j_2}, j_1)$.

KPS Characteristics

- Security — resilience against coalitions
- Connectivity — ability to find a key path between the pair
- Storage requirements — size of the node's key block
- Computational efficiency — complexity to compute a common key
- Scalability — ability to incorporate new nodes
- ...

The main challenge is construct a KPS with a 'good' trade-off

Security vs. Storage

KPS Resilience against Coalitions

Definition

A KPS is called *w-secure*, if for any pair of nodes i j and an arbitrary coalition of w colluders $\{k_1, \ldots, k_w\}$ such that $\{i, j\} \bigcap \{k_1, \ldots, k_w\} = \emptyset$, it holds that

$$H(\kappa_{ij}) = H\Big(\kappa_{ij} \Big| \bigcup_{m=1}^{w} \mathcal{S}_{k_m}\Big).$$

Typical Coalition Attacks against KPS

Find a coalition to

- attack a pairwise key =
  compromise a particular common key of a particular pair
- attack a node =
  compromise some node's key block (all node's keys)
- attack the scheme =
  compromise the system key pool

Blom's scheme

Description

- $\mathbf{D}$ — random symmetric $(w+1)\times(w+1)$ matrix over $GF(Q)$ — the global secret.
- $\mathbf{H}$ — $(w+1)\times N$ parity check matrix of RS-code over $GF(Q)$ — publicly available.
- Nodes' key blocks matrix

$$\mathbf{A} = \mathbf{DH} \tag{1}$$

— node j is given the column $\mathbf{a}_j$ of $\mathbf{A}$

- Pairwise key of i and j

$$\kappa_{ij} = \mathbf{h}_i^T \mathbf{a}_j = \mathbf{h}_i^T \mathbf{D} \mathbf{h}_j = \mathbf{h}_j^T \mathbf{a}_i, \tag{2}$$

Bloms's scheme

Properties

- Useful
  - every pair has a common key;
  - w-secure;
  - optimal in storage: $w+1$ keys for a node;
  - computationally efficient;
  - highly scalable: typically $N = Q \geqslant 2^{80}$.
- Features
  - all nodes are assumed to be equivalent:
    attacking coalition may include any $w+1$ nodes;
  - threshold scheme:
    no w colluders can get any pairwise key,
    any $w+1$ colluders get all keys.

attacking a pairwise key $\Leftrightarrow$ attacking a node $\Leftrightarrow$ attacking the scheme

Linear KPSs — Blom's Scheme Generalization

Idea: take other linear codes insead of RS-code.

Theorem (Sidel'nikov)

Let $\mathbf{H}$ *be* $n \times N$ *matrix over* $GF(Q)$*.*
The KPS given by (1) and (2) is w*-secure if and only if any* $w + 1$ *columns of* $\mathbf{H}$ *are linear independent over* $GF(Q)$*.*

Result: to construct w-secure KPS we need a parity check matrix of any $(N, N - n, w + 2)$ linear code — Linear KPS.

Linear KPSs — Useful research tool

Corollary

The pairwise key κ_{ij} of nodes i and j is compromised by a coalition $(\ell_1, \ldots, \ell_c)$ if and only if the columns $\mathbf{h}_i$ or $\mathbf{h}_j$ or both are linear dependent on the columns $\mathbf{h}_{\ell_1}, \ldots, \mathbf{h}_{\ell_c}$.

Corollary

The node j is compromised by a coalition $(\ell_1, \ldots, \ell_c)$ if and only if the column $\mathbf{h}_j$ is linear dependent on the columns $\mathbf{h}_{\ell_1}, \ldots, \mathbf{h}_{\ell_c}$.

Problem: find $\mathbf{H}$ suitable for a KPS for a particular network model.

Groups of Nodes

A group of nodes — is a subset of nodes enjoying a common property

- availbale computational resources / memory;
- communication abilities;
- physical resilience;
- geographical location;
- deployment time;
- nodes' roles;
- ...

Attacking Strategies against Groups

Adversary compromises nodes randomly and uniformly choosing them from

- the whole network without group restrictions — whole network attack.
- particular (predefined or fixed) groups — group-bounded attack.

Distribution of colluders among groups: in a coalition $(s_1, s_2, \ldots, s_u)$ there are s_1 colluders from group 1, s_2 colluders from group 2, etc.

Matrix **H** for Independent Groups

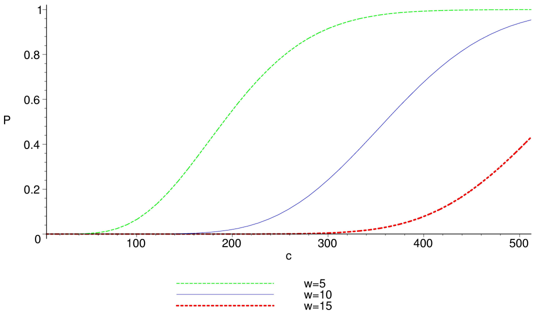
- There are u groups: in group ℓ there are N_ℓ nodes, $\sum_{\ell=1}^{u} N_\ell = N$.
- $\mathbf{H}_\ell$ — $(w_\ell + 1) \times N_\ell$ parity check matrix of a $(N_\ell, N_\ell - w_\ell - 1, w_\ell + 2)$ MDS-code over $GF(Q)$
- The nodes from group ℓ correspond to the columns of $\mathbf{H}_\ell$.
-

$$\mathbf{H}_{ind} = \begin{pmatrix} \mathbf{H}_1 & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_2 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{H}_3 & \dots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_u \end{pmatrix} \tag{3}$$

Independent Groups: Whole Network Attack

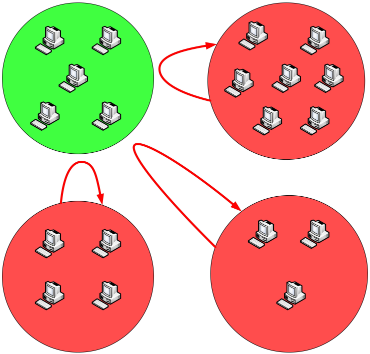
- The scheme is w-secure: $w = \min_\ell w_\ell$.
- Any $(w_1 + 1, w_2 + 1, \ldots, w_u + 1)$-coalition compromises any node.
- The probability to compromise a node from group ℓ by c colluders is

$$P(\ell, c) = \frac{\binom{N_\ell}{w_\ell+1}\binom{N-N_\ell}{c-w_\ell-1}}{\binom{N}{c}}.$$



Independent Groups: Group-Bounded Attack

A coalition can compromise a node from a group if there are at least $w_\ell + 1$ colluders from that group. $\rightarrow$
Links among nodes in the group is fully isolated from other groups.



Matrix $\mathbf{H}$ for Hierarchical Groups

- Level (group) 1 — the highest (most secure) level,
  level u — the lowest (least secure) level.
- $\mathbf{H}_0 = [z_j h_j^{i-1}]$ — parity check matrix of a GRS code.
- Split $\mathbf{H}_0$:
  by layers — $w_i + 1$ rows in a layer;
  by levels — N_j columns in a level.
  $\mathbf{H}_{ij}$ — $(w_i + 1) \times N_j$ matrix.
- Zeroize all matrix-blocks over the main diagonal in $\mathbf{H}_0$

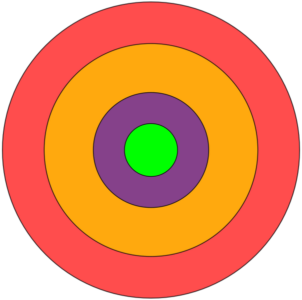
$$\mathbf{H}_{hrc} = \begin{pmatrix} \mathbf{H}_{11} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H}_{21} & \mathbf{H}_{22} & \dots & \mathbf{0} \\ & & \ddots & \\ \mathbf{H}_{u1} & \mathbf{H}_{u2} & & \mathbf{H}_{uu} \end{pmatrix} \qquad (4)$$

Hierarchical Groups: Whole Network Attack

- Any $(w_1 + 1, w_2 + 1, \ldots, w_u + 1)$-coalition compromises any node.
- No $(w_1 + 1, \ldots, w_{\ell-1} + 1, w_\ell, w_{\ell+1} + 1, \ldots, w_u + 1)$-coalition can compromise a node at level ℓ.

Hierarchical Groups: Group-Bounded Attack

- To compromise a node at level ℓ by a coalition from level ℓ only at least $\sum_{i=\ell}^{u}(w_i + 1)$ colluders are required. $\rightarrow$ Hierarchy of levels by internal security.
- To compromise a node at level ℓ by a coalition from level ℓ or lower it is required at least $w_\ell + 1$ colluders from level ℓ. $\rightarrow$ Higher levels are isolated from lower levels.



Thank you for your attention!
Questions?