A Collusion Attack on Pairwise Key Predistribution Schemes for Distributed Sensor Networks

Tyler W Moore

University of Cambridge
Computer Laboratory

IEEE Workshop on Pervasive Computing and Communications Security 2006
Pisa, Italy

UNIVERSITY OF CAMBRIDGE

Introduction

- Key predistribution schemes considered the safest way to bootstrap trust in a sensor network
- Main drawback: high storage overhead
- Key predistribution can actually be quite insecure
  - Many pre-loaded global secrets strengthen attacker incentive
  - Localised communication helps hide misbehaviour
- We describe an attack where colluding nodes reuse selected pairwise keys to create many false identities and hijack majority of communications

Bootstrapping a sensor network

- Constraints for establishing secure communication
  - Sensors deployed in hostile environments $\Rightarrow$ global passive adversary
  - No tamper-resistant hardware $\Rightarrow$ several corrupt nodes
  - Network topology unknown prior to deployment
  - No access to centralised server, trusted third party, etc.
- Solution
  - Assign keys to nodes in advance
  - Must balance security against storage and computing limitations of sensors

UNIVERSITY OF CAMBRIDGE

Options for predistributing keys

- Single master key predistribution
  - Inexpensive but susceptible to single compromise
- Pairwise key predistribution
  - Resilient to widespread compromise but storage infeasible for large networks (requires $n-1$ keys per node)
- Random key predistribution (Eschenauer & Gligor CCS 2002)
  - Nodes are assigned a random subset of keys from a large key space
  - If nodes share a common key, then a link can be established
  - Probabilistic guarantees based on random graph theory
  - Efficient, though fails badly when a small group of nodes are compromised

UNIVERSITY OF CAMBRIDGE

Options for predistributing keys (ctd.)

- Random pairwise scheme (Chan *et al.* IEEE S&P 2003)
  - Combines the random graph approach with pairwise key assignment
  - More efficient than pure pairwise scheme, but requires much more storage than EG 2003 (each node typically stores between $0.2n$ and $0.4n$ keys, depending on parameters)
  - No duplicate keys, so secure against eavesdropping attacks
  - Authors claim that pairwise key assignment enables mutual authentication at no added cost
- But is it secure from a colluding attacker?

UNIVERSITY OF CAMBRIDGE

Notation and system parameters

- Notation
  - n: Network size
  - n': expected number of neighbour nodes in radio range
  - p: probability of two nodes sharing a pairwise key
  - $N(d)$: set of neighbours of node d
  - $U(d)$: set of usable pairwise keys for node d
- System model
  - Nodes have limited communication radius
  - Nodes distributed uniformly across a space
  - Nodes pre-loaded with $n * p$ pairwise keys
  - Nodes broadcast their identifiers to neighbours, who check ID to see if they share a pairwise key

UNIVERSITY OF CAMBRIDGE

Attack preconditions

- Threat model
  - Attacker compromises a set of nodes A, $q = |A|$, obtaining keys and controlling all communications
  - Attacker nodes may collude across network via existing routing mechanism or an out-of-band channel
  - Attack targets the integrity and availability of communications
- Weaknesses of key predistribution
  - Many more secrets pre-loaded than actually used for communication ($n * p >> n'$)
  - Sensors have localised interactions, but global key assignment
- Key insight: colluding attackers can exploit latent secrets and communication gaps

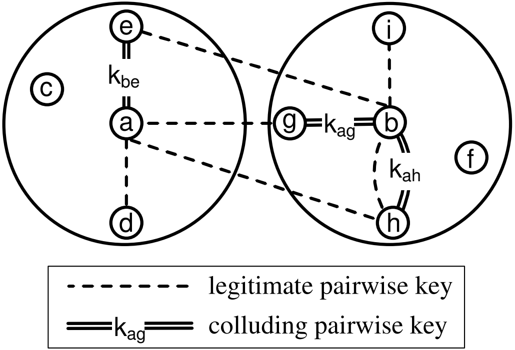
UNIVERSITY OF CAMBRIDGE

Attack description

- Consider two nodes controlled by an attacker, $a, b \in A$
  - a tells b its secrets
  - b masquerades as a to all of b's neighbours that a shares a pairwise key with, and vice versa
  - Repeat for all pairs of nodes in A
- As more nodes are compromised, more keys can be reused
- Like a Sybil attack (each node presents multiple identities)
- Like a node replication attack (multiple copies of same node)
- Attacker nodes pretend to be different nodes to different neighbours

UNIVERSITY OF CAMBRIDGE

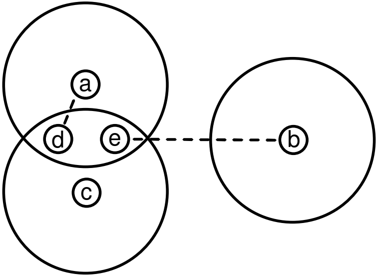
Example attack



	Independence	**Collusion**
$U(a)$	$\{k_{ad}\}$	$\{k_{ad}, k_{be}\}$
$U(b)$	$\{k_{bh}, k_{bi}\}$	$\{k_{bh}, k_{bi}, k_{ag}, k_{ah}\}$

UNIVERSITY OF CAMBRIDGE

Overlap



- Only one of nodes a and c should masquerade as b to node e
- Node c gains nothing by pretending to be a to d
- Overlap unavoidable as $q \rightarrow \frac{n}{n'}$

UNIVERSITY OF CAMBRIDGE

Attack Discussion

- Integrity, availability of communications targeted, not confidentiality
  - Many false channels can overwhelm legitimate ones
  - Authentication based on pairwise key possession inadequate
  - Node revocation, redundant routing schemes undermined
- Attack variables
  - Coordination levels: ratio $\frac{n'}{n}$ between average node neighbourhood and network size
  - Key storage: as p increases, more secrets can be exploited

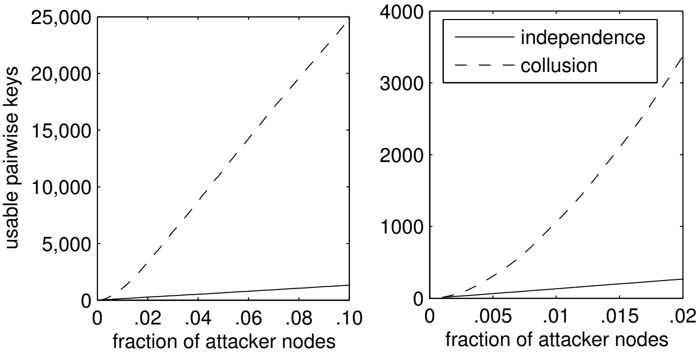
UNIVERSITY OF CAMBRIDGE

Impact Analysis & Measurement

- We focus on the number of usable pairwise secret keys available to an attacker
  - A pairwise key is usable if it is shared between nodes in communication range and it is not already in use within this range
- Attack Metrics
  - Number of usable pairwise keys available to a colluding attacker
  - Ratio of usable keys for attacker to keys available to attacker's neighbours
- Simulations
  - Nodes uniformly distributed over a plane
  - $n = 1000$, $n' = 60$, $p = .25$ and varied q, averaging results from 20 rounds

UNIVERSITY OF CAMBRIDGE

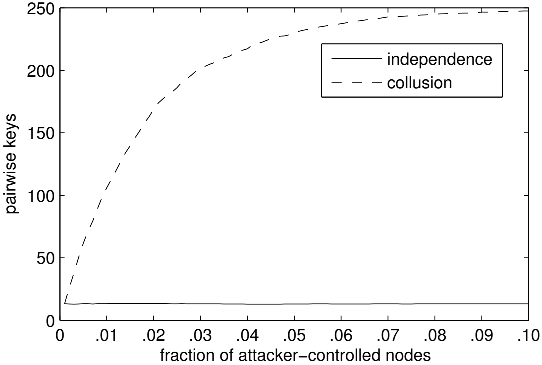
Increased usable pairwise keys



Measures $\sum_{a \in A} |U(a)|$ for increasing q

UNIVERSITY OF CAMBRIDGE

Per-node usable pairwise keys



As q grows large, each colluding node can establish $n * p$ fake communication channels

UNIVERSITY OF CAMBRIDGE

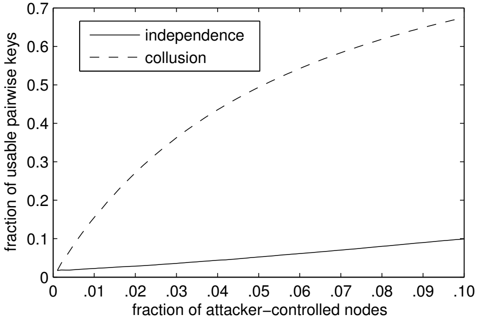
Quantifying attacker penetration

- But what is the overall impact of a collusion attack?

$$I(A) = \frac{\sum_{a \in A} |U(a)|}{\sum_{a \in A} \sum_{b \in N(a)} |U(b)|}$$

- $I(A)$ compares the number of usable pairwise keys available to an attacker to the keys available to attacker-controlled nodes' neighbours
- $I(A)$ reveals the fraction of working communication channels controlled by the attacker

Quantifying attacker penetration (ctd.)



- Corrupting 5% of nodes grants power to half of communication channels
- Any application requiring honest interaction with majority of neighbours is susceptible

UNIVERSITY OF CAMBRIDGE

Storage requirements

- How can colluding nodes actually store extra keys?
  - $n * p$ keys predistributed
  - Up to $n * p$ additional keys from collusion
  - Storing twice as many keys is too onerous
- Attack optimisation
  - Pairwise keys can only be used once by definition
  - After a node shares a pairwise key with another attacker-controlled node, it can delete the key and replace it with keys from the other node
  - So key-sharing becomes key-swapping
  - Attacker nodes still store no more than $n * p$ keys

UNIVERSITY OF CAMBRIDGE

Countermeasures

- Reduce value of compromised nodes to attackers
  - Discard unused keys after initialisation phase
    - No new nodes may join after initialisation
  - Reduce the number of pre-loaded keys
    - Exploit geographical proximity (topology foreknowledge)
    - Key infection (weaker attacker model)
- Detection mechanisms
  - Count connected neighbours
    - For normal usage, should share keys with $n' * p$ neighbours
    - Attacked node may have up to $q * p$ more
    - Identifying which neighbours are lying is difficult
  - Require nodes to transmit locations
    - Key reuse may be detected if nodes recursively ask neighbours for nodes' locations (Parno *et al. 2005*)
    - Location broadcast identifies new targets
    - Significant storage and transmission costs

UNIVERSITY OF CAMBRIDGE

Conclusions

- We have presented a collusion attack on the class of pairwise key predistribution schemes
- Small fraction of compromised nodes required to control majority of communication channels
- We question the wisdom of assigning global secrets to locally-communicating nodes
- More research is needed for pairing limited secrets to localised interactions
- For more, visit `http://www.cl.cam.ac.uk/~twm29/`

UNIVERSITY OF CAMBRIDGE