Markov Model-Directed Key Exchange

Paul L. Yu (US Army Research Lab), John S. Baras (ISR/ECE), Brian M. Sadler (ARL)
paul.yu@arl.army.mil, baras@isr.umd.edu, bsadler@arl.army.mil

Abstract

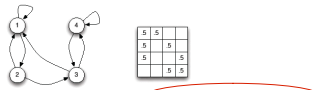
The replacement of secret keys is a central problem in key management. Typical solutions involve handshaking messages, complex computations, or trusted third parties. We introduce a novel key replacement method that exploits the randomness of Markov models to efficiently provide fresh keys to the users. Unlike other methods, the proposed method removes the need for extra communications or third parties while having comparable computational requirements, perfect forward secrecy, and resistance to known-key attacks.

Introduction

- Scenario: Alice and Bob share a secret symmetric key, but need to replace it with a new one.
- Possible key exchange methods:
  - Diffie-Helman key exchange (requires authentication to prevent MiM)
  - Public key infrastructure (requires third party cooperation)
  - Both require dedicated key exchange messages
- Proposed method:
  - Does not have expensive computational requirement
  - Does not require presence of third parties
  - Requires no dedicated messages

Example

- Assume that the validity of a secret key can be tested, e.g., encryption followed by CRC check
- Keys are drawn from keyspace $\mathcal{K}$, where $K = |\mathcal{K}|$
  - Without information from Alice, Bob has to check up to K keys to regain synchrony
  - Give Bob some assistance, but without communication
- Let Alice and Bob have identical Markov Models
  - Each state represents a key
  - State transitions dictate subsequent keys



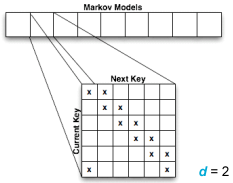
Valid sequence: 1, 1, 2, 3

Invalid sequence: 1, 2, 3, 2

- With the model, Bob has a *limited search space* for new key

Multiple Models

- Alice and Bob choose from a collection of Markov models
- Let there be L models and K keys
- Assumption: given the current key, the set of possible replacement keys has size d



$d = 2$

Complexity

- Communication:
  - No dedicated key exchange messages required:
    - Alice and Bob agree upon key exchange times *a priori*
    - Alice changes keys; Bob detects change and begins search
- Computation:
  - With d possible next keys, up to d decryptions/integrity checks are necessary to recover the correct key, with $d/2$ on average
  - Symmetric decryptions much cheaper than asymmetric
- Memory/Storage:
  - There are L models that Alice and Bob can choose from
  - Each Markov model requires $O(dK)$ storage space; total $O(dLK)$
  - Even with small keys, this is prohibitively large.
    - With d = 2, storing a single model with 32-bit keys requires ~ 1 GB
    - $L = K = 2^{32}$ requires ~ 4.3 billion gigabytes!

Storage Reduction

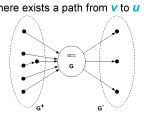
- In operation, Alice and Bob only require $O(d \log_2(K))$
  - current key
  - set of possible next keys
  - transition probabilities. *Assuming equiprobable transitions eliminates the storage requirement.*
- Random access method makes this possible
  - Query oracle to find set of next keys given current key
  - Algorithm:
    - Assumption: m-bit keys
    - Seed PRNG with function of current model l and current key i
      Example: seed can be $Hash(2^{m}l+i)$
    - Until there are d unique keys, select m-bit chunks of the output as possible next keys
    - Set transition probabilities of each candidate to be $1/d$

Security Properties

- Without knowing which model Alice and Bob are using, the adversary should **not** be able to determine:
  - the current key
  - the next key
  - the model
- Thus,
  - For almost any key in any model, the reachable key subspace should be large
  - Knowing the current key should not help Eve:
    - determine the next key
    - determine which model is being used
- Immediately, we require
  - The keyspace size K should be large
  - The generated key sequences should be aperiodic

Random Digraphs

- With the random access model, we cannot guarantee connectivity of the resulting key graph
- Fixed d implies model is a random digraph with constant out-degree
- *"For almost any key in $\mathcal{K}$, the reachable subspace should be large"*
  - Translation: Pick a random key in any model. The number of keys that can be eventually chosen should be large (near K)
  - Each model should have a single Giant Connected Component (GCC), from which any randomly chosen pair of keys u, v satisfies:
    - There exists a path from u to v
    - There exists a path from v to u



Size of GCC

d	% of K	Bit Penalty
2	.7972	.3369
3	.9408	.0881
4	.9803	.0287
5	.9931	.0100
6	.9975	.0036

C. Cooper and A. Frieze, "The size of the largest strongly connected component of a randomdigraph with a given degree sequence", Combinatorics, Probability, and Computing, May 2004.

Key Entropy

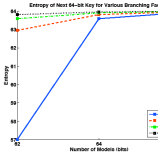
- Irreducible and aperiodic Markov chain converges to stationary distribution μ with entropy rate

$$H(\mathcal{X}) = -\sum_{m,n \in \mathcal{G}} \mu_m A_{mn} \log A_{mn} \leq \log d \qquad A_{mn} = 1/d$$

  - This is the entropy rate *as seen by Alice and Bob*
- What is the entropy of next key given current key? (Model not known)
  - L random models, K keys, d non-zero transition probabilities per key

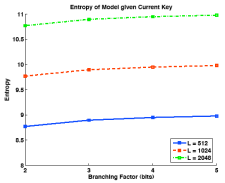
$$\bigcup_{\text{All models}} \text{Set of next keys from key } i$$

  - Aggregate key transitions across models
  - Allow duplicates
  - # duplicates modeled as Poisson process
  - Draw member of set with probability $1/dL$
  - dL should be greater than ~$2K$ for sufficient entropy
  - Eve's key entropy is ~ $\log_2(K)$ for large dL



Model Entropy

- Thus, increased branching factor d improves model entropy even when the current key is discovered

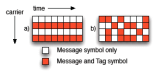


- Trades model entropy for receiver computation

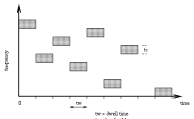
Wide Application Space

- Any scenario requiring secret keys
  - Message authentication codes
  - High rate encryption/decryption

- Physical layer authentication
  - Vary authentication structure over time
  - Enables rapid and low cost key switching



- Frequency hopped communications
  - Determine hopping sequence
  - Sequences no longer periodic!



Conclusion

- Novel key exchange method
  - No additional communications overhead
  - Low computation complexity
  - Low storage requirements
  - Good security properties
- Increasing the branching factor d:
  - Increases the size of reachable keyspace (confusion to adversary)
  - Improves key and model entropy to adversary (security)
  - Increases computation requirement of intended receiver (key entropy rate)

Relevant Publications/Awards:

•P.L. Yu, "Physical Layer Security", Ph.D. thesis, 2008.
•P.L. Yu, J.S. Baras, and B.M. Sadler, "Key Exchange Using Markov Models", *ACM Transactions on Information and System Security, submitted.*
•P.L. Yu, J.S. Baras, and B.M. Sadler, "Key Exchange Method and System using Markov Models", *US Provisional Patent filed 2008.*
•P.L. Yu, J.S. Baras, and B.M. Sadler, "Efficient Key Exchange for Symmetric Cryptosystems", *2008 Invention of the Year*, Category of Information Science.