Paths through Well-Behaved Bundles

(Abstract)

Joshua D. Guttman and F. Javier Thayer Fábrega
The MITRE Corporation
{guttman,jt}@mitre.org

June 22, 2000

The purpose of this abstract is to describe a new method for reasoning about cryptographic protocols [2] within the strand space model [4]. We have used this method to prove protocols correct and to identify flaws in them [1]; we have also used it to study interference between different protocols, deriving a broadly applicable way to show that the security of one protocol is independent of whether another protocol is in use [3].

The method has two main ingredients. First, we focus on paths. A path is a sequence of nodes[1] where $n \longmapsto n'$ is in the sequence only if

1. either n transmits a term t and n' receives the same term immediately from it, written $n \rightarrow n'$;

2. or n comes before n' on the same strand[2], written $n \Rightarrow^{+} n'$, and moreover n is a negative message reception and n' is a positive message transmission.

Some paths of interest trace a value from a node at which it originates to some node at which it is used. Indeed, whenever n is a node containing some value a, there must exist some path $p = p_1 \longmapsto \cdots \longmapsto p_k$ such that a originates at p_1, and every node p_i along the path contains a. Paths of this kind can be used to study the pedigree by which a value reaches some later node; we will call them " pedigree paths."

Other paths of interest follow the penetrator's transformations of a term from the time it is received from a positive regular node to the time it is delivered to a negative regular node. By studying the possible forms of such paths, we may examine the range of effects that the penetrator may have on a term. A

[1]Each node n is either a message transmission, called a positive node, or a message reception, called a negative node.

[2]A strand is a sequence of nodes consisting of successive actions by a single principal is a single run. The relation $n \Rightarrow n'$ means that n' is the next node in the sequence after n.

penetrator path is a path $p = p_1 \longmapsto \cdots \longmapsto p_i \longmapsto \cdots \longmapsto p_k$ such that every node p_j is a penetrator node, except possibly if $j = 1$ and $j = k$.

The second main ingredient in our method is to focus on certain kinds of well-behaved bundles[3] in which paths are more predictable. We introduce an equivalence relation on bundles in [2], according to which two bundles are equivalent if they have the same regular nodes. The penetrator nodes of equivalent bundles may differ, and the relations $n \to n'$ of transmitter to receiver may differ between the two bundles.

Authentication and secrecy goals for authentication and key distribution protocols may be expressed in a form that is invariant under this equivalence relation. That is, if $\mathcal{C}$ is a bundle satisfying a goal, and $\mathcal{C}'$ is equivalent to $\mathcal{C}$, then $\mathcal{C}'$ satisfies that goal also. Put the other way round, if $\mathcal{C}'$ is a counterexample, then so is $\mathcal{C}$. If we are looking for a counterexample to a security goal, and we know that every bundle has an equivalent bundle of a special form, then it is enough to look for a counterexample of that special form.

Moreover, there are a number of useful special forms for bundles, such that every bundle is equivalent to a bundle in the special form. A bundle is *normal* if, for every penetrator path p, every destructive penetrator action along p precedes every constructive penetrator action along p.[4] Every bundle is equivalent to a normal bundle [2, Proposition 3.8].

To understand the next special form, suppose that a node m contains concatenated all the pieces from which the term of a negative node n is also concatenated. If the penetrator can receive these pieces directly from m, then he can deliver them in the right (re-concatenated) form to n. The penetrator does not need any help from regular participants to do this. A bundle is *efficient* if this never happens. That is, it is efficient if, whenever a node m contains concatenated all the pieces from which the term of a negative node n is also concatenated, then there is no regular node m' such that $m \prec_{\mathcal{C}} m' \prec_{\mathcal{C}} n$. Every bundle is equivalent to an efficient bundle [2, Proposition 3.22].

There are 4 advantages to this approach:

1. The focus on paths through bundles gives a strongly geometrical flavor to reasoning about protocols, suggesting many new results.

[3] A bundle is a finite graph consisting of nodes and arrows of both kinds $\to$ and $\Rightarrow$, which is causally well-founded. That means that it is acyclic, and closed backwards for both kinds of arrow. A bundle represents a possible history in which one or more principals participate in (possibly mismatched) protocol runs. In a bundle $\mathcal{C}$, there is a partial order $\prec_{\mathcal{C}}$ such that $n \prec_{\mathcal{C}} n'$ whenever there is a sequence of arrows $\to$ and $\Rightarrow$ leading from n to n'.

[4] The basic penetrator actions fall into three groups. Some initiate a value, either a key or a text known to the penetrator or guessed by him. Some actions break down a compound term, either decrypting a ciphertext using the matching key or separating a concatenated term into parts. Finally, some actions construct a new compound term, either encrypting a plaintext using a key or concatenating two parts. In a normal bundle, the penetrator never constructs a compound term just to take it apart again.

2. The efficiency property plays roughly the role of an induction principle, since it guarantees that the node n comes immediately after m (measured in intervening regular nodes).

3. Certain penetrator paths in normal bundles have a subterm property, meaning that $\mathrm{term}(p_i) \sqsubset \mathrm{term}(p_1)$ and $\mathrm{term}(p_i) \sqsubset \mathrm{termterm}(p_k)$, where p_k is the last node on p, and p_i is the node on p that comes after all destructive penetrator actions and before all constructive penetrator actions.[5] This property allows us to predict which terms may occur in p. It provided the original motivation for [3].

4. If a value v originates uniquely on a regular strand, and is later received back on that strand in cryptographically altered form, then we may infer that there is a pedigree path p leading from the earlier node to the later node. The cryptographic forms in which v occurs at the beginning and end of p may allow us to infer that a regular participant—rather than the penetrator—must have altered it. This idea provides a rigorous justification for a common strategy in protocol design, and motivated the idea of authentication tests [1].

In this talk, we will describe these ideas in more detail, and summarize some of the techniques for reasoning about cryptographic protocols to which they lead.

References

[1] Joshua D. Guttman and F. Javier THAYER Fábrega. Authentication tests. In *Proceedings, 2000 IEEE Symposium on Security and Privacy*. May, IEEE Computer Society Press, 2000.

[2] Joshua D. Guttman and F. Javier THAYER Fábrega. Authentication tests and the normal penetrator. MTR 00B04, The MITRE Corporation, February 2000. Also submitted for publication.

[3] Joshua D. Guttman and F. Javier THAYER Fábrega. Protocol independence through disjoint encryption. In *Proceedings, 13th Computer Security Foundations Workshop*. IEEE Computer Society Press, July 2000.

[4] F. Javier THAYER Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(2/3):191–230, 1999.

[5] We call this node p_i the *bridge* of the path p; in a normal bundle, every penetrator path has exactly one bridge [2, Proposition 3.14].