

Untraceability of RFID Protocols

Ton van Deursen, Sjouke Mauw, and Saša Radomirović

University of Luxembourg



Radio frequency identification (RFID)

Introduction

-RFID

-Radio frequency

identification (RFID)

-Security requirements

-Motivation

Untraceability

Examples

Conclusion

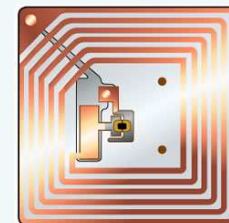
Backend



Reader



Tag



Secure channel



Insecure channel



Radio frequency identification (RFID)

Introduction

-RFID

-Radio frequency
identification (RFID)

-Security requirements

-Motivation

Untraceability

Examples

Conclusion

RFID tags

- are very small,
- can be mass-produced,
- can communicate wirelessly,
- carry a unique identification number.



Security requirements

Introduction

-RFID
-Radio frequency
identification (RFID)

-Security requirements

-Motivation

Untraceability

Examples

Conclusion

A minimal requirement for the RFID setting is **authentication**: a tag must provide evidence to a reader that he is who he claims to be.



Security requirements

Introduction

-RFID
-Radio frequency
identification (RFID)

-Security requirements
-Motivation

Untraceability

Examples

Conclusion

A minimal requirement for the RFID setting is **authentication**: a tag must provide evidence to a reader that he is who he claims to be.

The notion of **recent aliveness** of the tag as authentication property suffices. Recent aliveness guarantees that during a protocol execution of the reader, a tag has generated a message.



Security requirements

Introduction

-RFID
-Radio frequency
identification (RFID)

-Security requirements

-Motivation

Untraceability

Examples

Conclusion

Because of the travelling nature of RFID tags, care should be taken that the privacy of the carrier of the tag is protected. An adversary should not be able to trace a tag through space and time.



Security requirements

Introduction

-RFID
-Radio frequency
identification (RFID)

-Security requirements

-Motivation

Untraceability

Examples

Conclusion

Because of the travelling nature of RFID tags, care should be taken that the privacy of the carrier of the tag is protected. An adversary should not be able to trace a tag through space and time.

Therefore, a second requirement on RFID protocols is **untraceability** of the tag, ensuring that an adversary cannot recognize a tag he previously observed.



Introduction

-RFID
-Radio frequency
identification (RFID)
-Security requirements

-Motivation

Untraceability

Examples

Conclusion

Eavesdropping on messages is easy:

- Communication is contactless
- No clear line-of-sight is necessary
- Messages are broadcasted



Motivation

Introduction

-RFID
-Radio frequency
identification (RFID)
-Security requirements

-Motivation

Untraceability

Examples

Conclusion

Eavesdropping on messages is easy:

- Communication is contactless
- No clear line-of-sight is necessary
- Messages are broadcasted

A formal definition of untraceability is needed:

- Untraceability has typically been treated rather informally.
- No formal definition has been proposed up to now.



Approach

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Intuitively, a protocol is said to be **untraceable** if an adversary cannot recognize a tag he previously observed.



Approach

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Intuitively, a protocol is said to be **untraceable** if an adversary cannot recognize a tag he previously observed.

We define untraceability as a trace property of a role of the protocol.



Approach

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Intuitively, a protocol is said to be **untraceable** if an adversary cannot recognize a tag he previously observed.

We define untraceability as a trace property of a role of the protocol.

If there is a trace for the protocol in which there are two communications with the **same tag**, we find a trace in which one of these communications is replaced by a communication with a **different tag**.



Reinterpretation

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

The notion of **reinterpretation** will be used to express that subterms of a message can be substituted by other terms if the adversary is not able to read (or interpret) these subterms. All terms that the adversary can interpret remain unchanged. The notion of reinterpretation was first introduced by Garcia *et al.*



Reinterpretation

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

The notion of **reinterpretation** will be used to express that subterms of a message can be substituted by other terms if the adversary is not able to read (or interpret) these subterms. All terms that the adversary can interpret remain unchanged. The notion of reinterpretation was first introduced by Garcia *et al.*

Definition (reinterpretation) *A map π from run terms to run terms is called a reinterpretation under knowledge set M if it and its inverse π^{-1} satisfy the following conditions:*

$$\pi(m) = m$$

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

$$\pi(f(m)) = f(\pi(m))$$

if m is a basic run term

if $m = (m_1, \dots, m_n)$ is an n -tuple

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

if $M \vdash m$

or f is not a hash function.



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 1: Let $\pi = \{\{m\}_k \mapsto \{m'\}_k\}$ for $M = \{k^{-1}\}$. Is π a reinterpretation?



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 1: Let $\pi = \{\{m\}_k \mapsto \{m'\}_k\}$ for $M = \{k^{-1}\}$. Is π a reinterpretation?

$$\pi(m) = m$$

if m is a basic run term

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

if $m = (m_1, \dots, m_n)$ is an n -tuple

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

$$\pi(f(m)) = f(\pi(m))$$

if $M \vdash m$

or f is not a hash function.



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 1: Let $\pi = \{\{m\}_k \mapsto \{m'\}_k\}$ for $M = \{k^{-1}\}$. Is π a reinterpretation?

$$\pi(m) = m$$

if m is a basic run term

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

if $m = (m_1, \dots, m_n)$ is an n -tuple

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

$$\pi(f(m)) = f(\pi(m))$$

if $M \vdash m$

or f is not a hash function.



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 1: Let $\pi = \{\{m\}_k \mapsto \{m'\}_k\}$ for $M = \{k^{-1}\}$. Is π a reinterpretation?

$$\pi(m) = m$$

if m is a basic run term

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

if $m = (m_1, \dots, m_n)$ is an n -tuple

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

$$\pi(f(m)) = f(\pi(m))$$

if $M \vdash m$

or f is not a hash function.

No, by the third condition $\pi(\{m\}_k) = \{\pi(m)\}_k$, should hold. This violates the first condition, since $\pi(m) = m'$



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 2: Let $\pi = \{h(m, n) \mapsto h(m, n')\}$ for $M = \{m\}$. Is π a reinterpretation?



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 2: Let $\pi = \{h(m, n) \mapsto h(m, n')\}$ for $M = \{m\}$. Is π a reinterpretation?

$$\pi(m) = m$$

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

$$\pi(f(m)) = f(\pi(m))$$

if m is a basic run term

if $m = (m_1, \dots, m_n)$ is an n -tuple

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

if $M \vdash m$

or f is not a hash function.



Reinterpretation (example)

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Example 2: Let $\pi = \{h(m, n) \mapsto h(m, n')\}$ for $M = \{m\}$. Is π a reinterpretation?

$$\pi(m) = m$$

if m is a basic run term

$$\pi(m) = (\pi(m_1), \dots, \pi(m_n))$$

if $m = (m_1, \dots, m_n)$ is an n -tuple

$$\pi(\{m\}_k) = \{\pi(m)\}_k$$

if $M \vdash k^{-1}$

or $M \vdash m \wedge M \vdash k$

$$\pi(f(m)) = f(\pi(m))$$

if $M \vdash m$

or f is not a hash function.

Yes, all four conditions are satisfied.



Indistinguishability of traces

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

Reinterpretations generalize in the obvious way to traces. We say that two traces are **indistinguishable** to the adversary, if the adversary cannot see any meaningful difference between the two traces, based on the knowledge he has.

Definition (indistinguishability of traces) *Let M be the adversary's knowledge at the end of trace t . The trace t is indistinguishable from a trace t' , denoted by $t \sim t'$, if there is a reinterpretation π under M , such that $\pi(t) = t'$.*



Untraceability

Introduction

Untraceability

- Approach
- Reinterpretation
- Indistinguishability of traces
- Untraceability

Examples

Conclusion

We assume that within a trace t the events belonging to a single protocol execution can be identified. We call the collection of these events a **subtrace**. We enumerate the non-empty subtraces according to their first observable event. The i -th subtrace of role R in trace t is denoted by t_i^R .



Untraceability

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

We assume that within a trace t the events belonging to a single protocol execution can be identified. We call the collection of these events a **subtrace**. We enumerate the non-empty subtraces according to their first observable event. The i -th subtrace of role R in trace t is denoted by t_i^R .

We say two subtraces t_i^R and t_j^R are **linked**, notation $L(t_i^R, t_j^R)$, if the agent executing the events in both subtraces is the same.



Untraceability

Introduction

Untraceability

-Approach

-Reinterpretation

-Indistinguishability of traces

-Untraceability

Examples

Conclusion

A protocol is **untraceable** if for every trace in the protocol, whenever there are two subtraces which are linked, another trace can be found in which the subtraces are not linked.



A protocol is **untraceable** if for every trace in the protocol, whenever there are two subtraces which are linked, another trace can be found in which the subtraces are not linked.

Definition (untraceability) *A protocol P is untraceable with respect to role R if*

$$\begin{aligned} & \forall t \in \text{Traces}(P) \\ & \forall_{i \neq j} L(t_i^R, t_j^R) \Rightarrow \\ & \exists t' \in \text{Traces}(P) t \sim t' \wedge \neg L(t'_i{}^R, t'_j{}^R). \end{aligned}$$



An untraceable protocol

Introduction

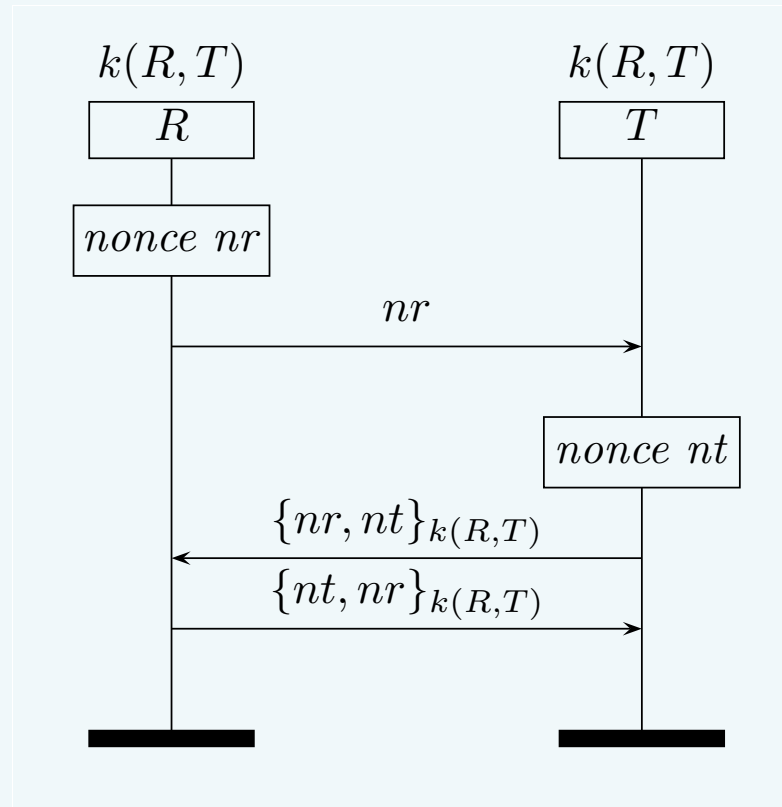
Untraceability

Examples

-An untraceable protocol

-A traceable protocol

Conclusion



Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong authentication for RFID systems using the AES algorithm (CHES 2004).



An untraceable protocol

Introduction

Untraceability

Examples

-An untraceable protocol

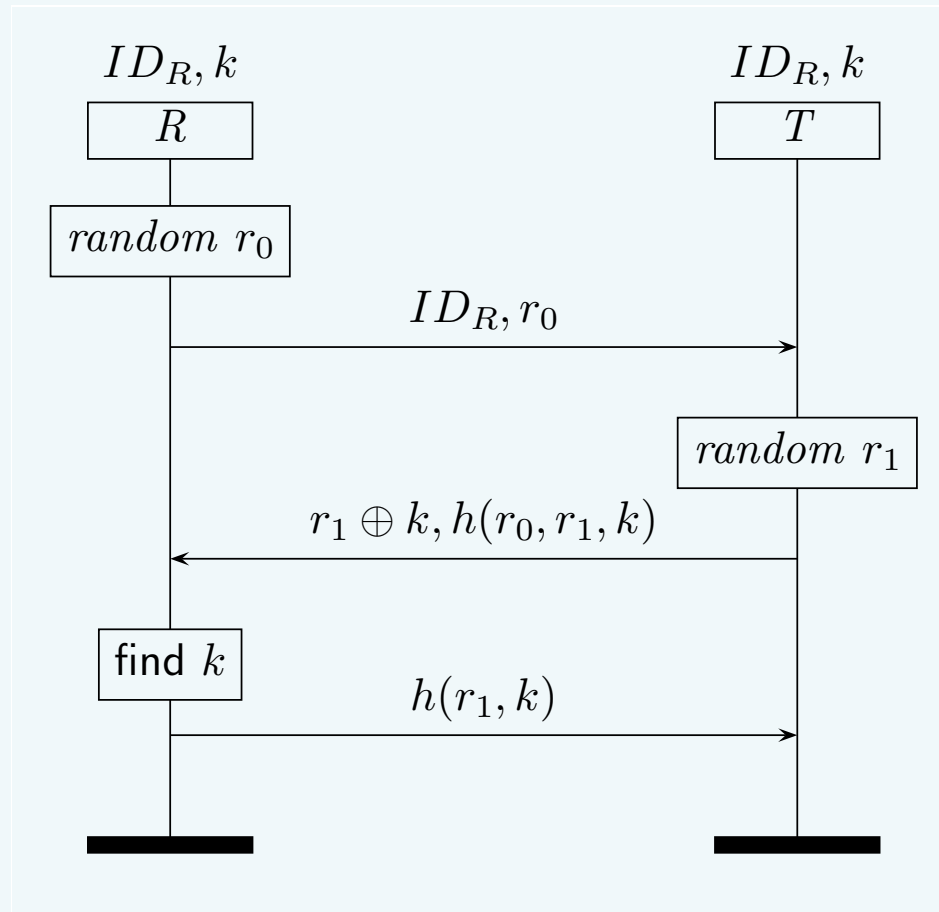
-A traceable protocol

Conclusion

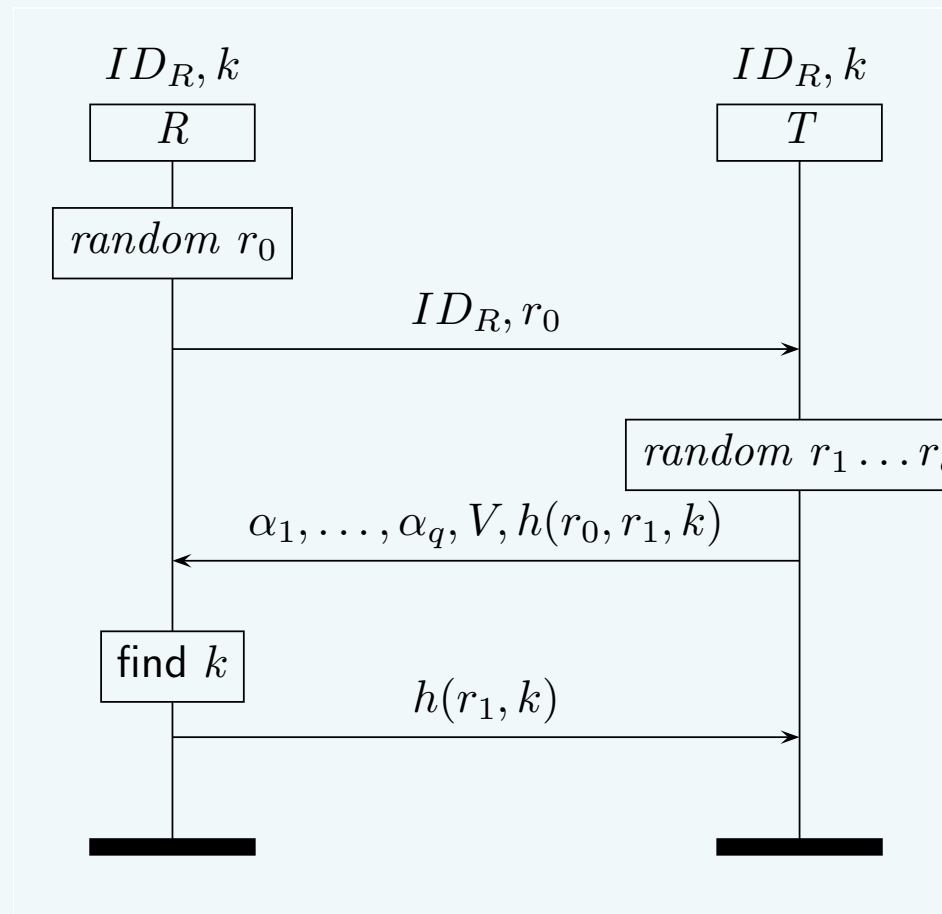
- Let t be a trace in which the tag role is twice executed by tag T1.
- We construct t' from t by replacing the messages from the first execution of tag T1 by messages from tag T2:

$$\begin{aligned}\pi(\{x, nt\}_{k(y, T1)}) &= \{x, nt\}_{k(y, T2)} && \text{for any } x \text{ and } y, \\ \pi(\{nt, x\}_{k(y, T1)}) &= \{nt, x\}_{k(y, T2)} && \text{for any } x \text{ and } y, \\ \pi(m) &= m && \text{elsewhere.}\end{aligned}$$

- π is a valid reinterpretation if nt and $k(R, T)$ are secret.
- By construction, the changes produce a valid trace.
- t' is a trace in which the tag role is executed by two different agents.



Di Pietro, R., Molva, R.: Information confinement, privacy, and security in RFID systems. In ESORICS 2007.



- Compute one-time-pad $\alpha_i = r_i \oplus k$ for every random number.

- Leak 1 bit of information using a hash-like function:

$$V[i] = DPM(r_i) =$$

$$M(r_i[1], r_i[2], r_i[3]) \oplus \dots \oplus M(r_i[\ell/3 - 2], r_i[\ell/3 - 1], r_i[\ell/3])$$



A traceable protocol

Introduction

Untraceability

Examples

-An untraceable protocol

-A traceable protocol

Conclusion

- The *DPM*-function leaks one bit of information.
- However, by combining the different α 's and *DPM*'s and using linear algebra more information can be gained.
- The key space is reduced from 2^ℓ to $2^{\ell/3}$ possible keys.
- The probability that two keys have the same key space is negligibly small.
- An attacker can recognize a tag he previously observed.



Contributions

Introduction

Untraceability

Examples

Conclusion

-Contributions

-Future work

Formal definition of untraceability

- Verify protocols correct or incorrect.
- Starting point for automated verification of untraceability.



Introduction

Untraceability

Examples

Conclusion

-Contributions

-Future work

- Refinements of the untraceability definition:
 - Weak untraceability.
 - Untraceability groups.
 - Forward untraceability.



Introduction

Untraceability

Examples

Conclusion

-Contributions

-Future work

- Refinements of the untraceability definition:
 - Weak untraceability.
 - Untraceability groups.
 - Forward untraceability.
- Reinterpretations of functions with algebraic properties



Introduction

Untraceability

Examples

Conclusion

-Contributions

-Future work

- Refinements of the untraceability definition:
 - Weak untraceability.
 - Untraceability groups.
 - Forward untraceability.
- Reinterpretations of functions with algebraic properties
- Automated verification of untraceability