A holistic approach to RFID security and privacy

Evangelos Rekleitis, Panagiotis Rizomiliotis, Stefanos Gritzalis

Department of Information and Communications Systems Engineering
University of the Aegean, Greece

SecIoT'10
1st International Workshop on the Security of the Internet of Things

IOT, RFID and security

- Build IOT security by designing from the start secure components
- Everyday objects tagged with low cost RFID tags will populate the IOT

RFID protocols class	**Hardware Requirements**
Full-fledged	Cryptographic operations (ECC in 4500+ gates equiv.)
Simple	Cryptographic one-way hash functions
Lightweight	Random number generator & simple functions (e.g. Cyclic Redundancy Code) checksum
Ultra-lightweight	Simple bitwise operations (e.g. XOR)

A set of security requirements

- Resistant to:
    - Tag impersonation
    - Reader impersonation
    - Denial of Service
- Tag anonymity:
    - Forward security
    - Backward security

Operations:

- Tag authentication
- Revocable access delegation
- Ownership transfer
- Permanent & temporal tag invalidation

- Economic restrictions

Policies: Problematic

Control tag resources with Access control mechanisms

- Static systems
  - ACL, RBAC...
- Dynamic environment (IOT)
  - ABAC/RuBAC
  - Policies

Tag's Life Cycle

- Creation
- Attachment
- Operation
- End-of-life

Policies: Open Issues

- Efficiency
- Policy and rule construction
- Access control complexity
- Privacy issues regarding use of attributes
- Interoperability

A protocol for secure tag management

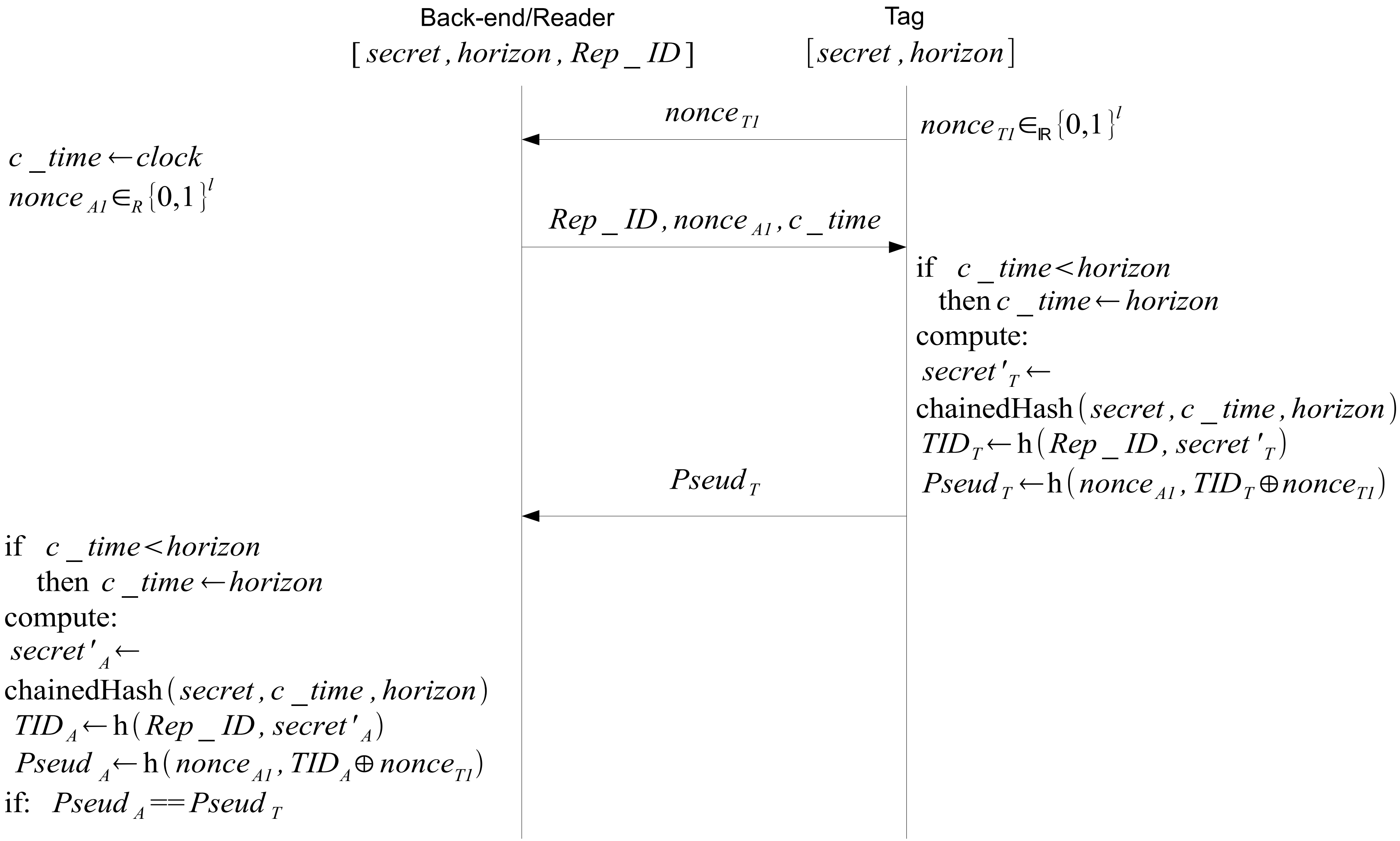
Goals

- Tag Authentication
- Delegated Tag Authentication
- Revocation of Tag Delegation
- Ownership Transfer
- *Plays well* with policies

Assumptions

- *Simple* tag (hash function, pRNG)
- Safe time slots
- Secure communication channel between the reader and the back-end system

Tag authentication



Back-end/Reader

$[\,secret, horizon, Rep\_ID\,]$

Tag

$[\,secret, horizon\,]$

$nonce_{T1} \in_{\mathbb{R}} \{0,1\}^l$

$nonce_{T1}$

$c\_time \leftarrow clock$

$nonce_{A1} \in_R \{0,1\}^l$

$Rep\_ID, nonce_{A1}, c\_time$

if $c\_time < horizon$

then $c\_time \leftarrow horizon$

compute:

$secret'_T \leftarrow$

chainedHash$(secret, c_time, horizon)$

$TID_T \leftarrow \mathrm{h}(Rep\_ID, secret'_T)$

$Pseud_T \leftarrow \mathrm{h}(nonce_{A1}, TID_T \oplus nonce_{T1})$

$Pseud_T$

if $c\_time < horizon$

then $c\_time \leftarrow horizon$

compute:

$secret'_A \leftarrow$

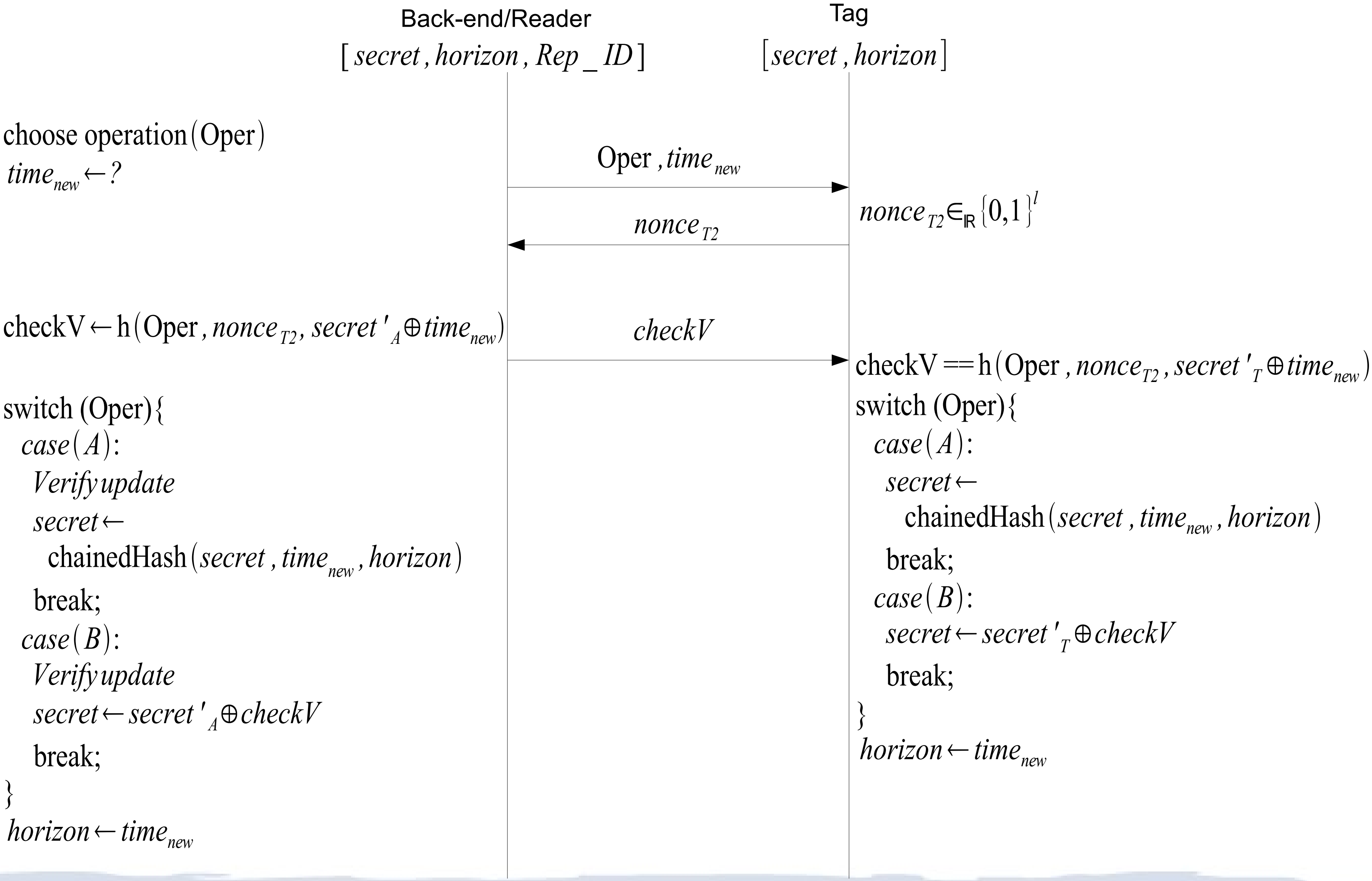
chainedHash$(secret, c_time, horizon)$

$TID_A \leftarrow \mathrm{h}(Rep\_ID, secret'_A)$

$Pseud_A \leftarrow \mathrm{h}(nonce_{A1}, TID_A \oplus nonce_{T1})$

if: $Pseud_A == Pseud_T$

Tag data update



Back-end/Reader

$[\,secret, horizon, Rep\_ID\,]$

Tag

$[\,secret, horizon\,]$

```
choose operation(Oper)
$time_{new} \leftarrow ?$
```

$\xrightarrow{\text{Oper}, time_{new}}$

$nonce_{T2} \in_R \{0,1\}^l$

$\xleftarrow{nonce_{T2}}$

```
$\text{checkV} \leftarrow \text{h}(\text{Oper}, nonce_{T2}, secret'_A \oplus time_{new})$
```

$\xrightarrow{checkV}$

```
$\text{checkV} == \text{h}(\text{Oper}, nonce_{T2}, secret'_T \oplus time_{new})$
switch (Oper){
  $case(A)$:
    $secret \leftarrow$
      $\text{chainedHash}(secret, time_{new}, horizon)$
    break;
  $case(B)$:
    $secret \leftarrow secret'_T \oplus checkV$
    break;
}
$horizon \leftarrow time_{new}$
```

```
switch (Oper){
  $case(A)$:
    $Verify update$
    $secret \leftarrow$
      $\text{chainedHash}(secret, time_{new}, horizon)$
    break;
  $case(B)$:
    $Verify update$
    $secret \leftarrow secret'_A \oplus checkV$
    break;
}
$horizon \leftarrow time_{new}$
```

Security Analysis

Attacker's arsenal

- Eavesdropping (*Weak-Passive*)
- Full control of network operations (*Weak-Active*)
- Tag corruption at end of attack (*Forward-Corruptive*)
- Destructive tag corruption (*Destructive-Corruptive*)
- Arbitrary tag corruption (*Strong-Corruptive*)

- *Side channel knowledge*

Security Analysis

- Tag & Reader impersonation
  - Against active attackers
- DOS/Desynchronization
  - Against active attackers
- Tag anonymity
  - Against active attackers
- Forward untraceability
  - Against strong attackers
- Backward untraceability
  - Using safe slots

Conclusions

- Effort on complete and low cost security solutions
- More research on the combination of dynamic *access control mechanisms* and *policies* in IOT environments
    - Efficiency, usability, interoperability etc.

Thank you very much