A Policy-driven Approach to Access Control in Future Internet Name Resolution Services

Xiruo Liu, Wade Trappe, Janne Lindqvist

Winlab, Rutgers University
Topic List

- Background
- MobilityFirst & Global Name Resolution Service (GNRS)
- Access Control in Global Name Resolution Service
  - Overview of access control in the GNRS
  - Spatio-temporal access control
  - Token format
  - Token usage discussion
Current Internet was developed without security or regulation as its core principals.

Solutions developed so far are basically patches added to Internet protocol stack.

Mobility becomes another trend of future Internet.

Separation of identifier and locator is proposed to handle mobility, such as Global Name Resolution Service (GNRS) in MobilityFirst.

Our goal: develop access control scheme for name resolution services to protect the information needed to launch an attack in a clean-slate future architecture design.
Global Name Resolution Service in MobilityFirst

- GNRS mapping:
  \(< \text{GUID, NA, T, E} >\)

- GNRS operations: insert, update, query.
Overview of Access Control in GNRS

- **Problem**
  - No protection for the mapping from being queried by illegitimate users.

- **Consequences**
  - Information/privacy leakage.
  - Attacks, e.g. DoS attack.
  - Track users’ behavior, etc.

- **Solution**
  - Integrating access control to the GNRS.

- **Benefits**
  - Protect mapping information from unauthorized access.
  - Support advanced services and fine-grained functionalities.
Overview of Access Control in GNRS

- **Access control language**
  - eXtensible Access Control Markup Language (XACML)
  - Can handle basic GNRS access control, identity-based access control (IBAC) and attribute-based access control (ABAC)

- **Policy format**
  - Basic format: \((GUID_B, T_B, E_B)_{A^{-1}}\)
  - Whitelist/backlist: \(\{(W, GUID_1, T_1, E_1), (B, GUID_2, T_2, E_2), \ldots\}_{A^{-1}}\)
Spatio-temporal Access Control in GNRS

- General Spatio-temporal access control (STAC)
  - Target
    - Grant the mapping based on spatio-temporal (ST) characteristics.
  - Challenge
    - A malicious user may lie about its location.
  - Current work
    - No guarantee for the correctness of the ST information.
    - Little support for the security of submission process
  - Solution
    - Incorporate ST verification to ensure the correctness of ST information.
    - Adopt various security mechanisms to secure the query process.
Spatio-temporal Access Control in GNRS
### Spatio-temporal Access Control in GNRS

1. **A → S:** \(\{(\text{GUID}_A, NA_1, T_A, E_A)_{A^{-1}}, (L, T, E)_{P_{\text{flag}}}\}\)
   - A is the mapping owner in network NA1, S is a GNRS server.
   - Policy \((L, T, E)\) contains location constraint \(L\) and two time constraints.

2. **B → S:** \(\{\text{GUID}_B, [\text{GUID}_S, N_1, (\text{GUID}_A, \text{GUID}_B)_{B^{-1}}]_S\}\)
   - User B sends a query request to the GNRS.

3. **S → B:** \(\{\text{GUID}_S, \{\text{GUID}_B, N_2, L_Q, T_Q\}_{S^{-1}}\}_B\)
   - Before evaluating the query request, S sends B a ST information request.

4. **B → AP1:** \(\{\text{GUID}_B, [\text{GUID}_{AP1}, (\text{GUID}_B, N_2 + 1, L_B, T_B)_{B^{-1}}]_{AP1}\}\)
   - B sends its ST information to its access point AP1 for authentication.

5. **AP1 → S:** \(\{\text{GUID}_{AP1}, [\text{GUID}_S, \text{GUID}_B, (\text{GUID}_B, N_2 + 1, L_B, T_B)_{B^{-1}}]_{AP1^{-1}}]_S\}\)
   - If B’s ST information is correct, AP1 also signs the ST response and then forwards it to S.

6. **S → B:** \(\{(\text{GUID}_A, NA_1, T_A, E_A)_{A^{-1}, NA_1^{-1}}, (N_1 + 1)\}_B\)
   - S submits the ST information for evaluation. If the access decision is “permit”, S replies B with A’s mapping.

---

ST verification
Spatio-temporal Access Control in GNRS

- Spatio-temporal access control with state transitions
  - Definition of state
    - Being at a specific location in a specific time interval.
    - Is represented by a location $L$ and time interval $(T, E)$ as $<L,T,E>$.
  - Target: A stateful form of access control
    - Accessibility to the mapping depends on not only the current state, but also the previous state.
  - Challenge
    - Scalability & efficiency issue: a large burden for distributed servers to maintain users’ state records in a large scale mobile network.
  - Solution
    - Introduce a token-based approach to handle the state verification process.
Spatio-temporal Access Control in GNRS

1. \(A \rightarrow S: \{(\text{GUID}_A, \text{NA}_1, T_A, E_A)_{A^{-1}}, [(L_1, T_{P_1}, E_{P_1}), (L_2, T_{P_2}, E_{P_2})]_{A^{-1}}, P_{\text{flag}}\}\)
   - The policy involves two states: the current state and previous state.

2. \(B \rightarrow S: \{\text{GUID}_B, [\text{GUID}_S, N_1, (\text{GUID}_A, \text{GUID}_B)_{B^{-1}}]_S\}\)
   - Mobile user B sends a query request to the GNRS.

3. \(S \rightarrow B: \{\text{GUID}_S, (\text{GUID}_B, N_2, L_Q, T_Q, TK_Q)_{S^{-1}}_B\}\)
   - Before evaluating the query request, S sends B a ST information request.

4. \(B \rightarrow \text{AP}_1: \{\text{GUID}_B, [\text{GUID}_{\text{AP}_1}, (\text{GUID}_B, N_2 + 1, L_B, T_B, TK_B)_{B^{-1}}]_{\text{AP}_1}\}\)
   - B presents its current valid token TK\(_B\) to \(\text{AP}_1\) for ST authentication.

5. \(\text{AP}_1 \rightarrow S: \{\text{GUID}_{\text{AP}_1}, [\text{GUID}_S, \text{GUID}_B, (\text{GUID}_B, N_2 + 1, L_B, T_B, TK_B)_{B^{-1}}_{\text{AP}_1^{-1}}]_S\}\)
   - If B’s ST information is correct, \(\text{AP}_1\) also signs the ST response and then forwards it to S.

6. \(S \rightarrow B: \{(\text{GUID}_A, \text{NA}_1, T_A, E_A)_{A^{-1}, \text{NA}_1^{-1}}, (N_1 + 1)(TK'_B)\}\)
   - S submits the ST information for evaluation. If the access decision is “permit”, S replies B with A’s mapping together with a new token TK\(_B'\) for B’s future use.
Spatio-temporal Token Discussion

- **Features of ST token design**
  - Satisfy the advanced requirements for multiple previous states.
  - Robust to potential attacks.
  - Be able to express some special policies.

- **Token format**

  \[
  \{Seq, GUID, S_P, S_C, T_T, E_T\}_K
  \]

  - Seq: token sequence number.
  - GUID: the identifier of the user that the token belongs to.
  - S_P: the user’s previous state.
  - S_C: the user’s current state.
  - T_T: token generation time.
  - E_T: token expiration time.
  - K: a key submitted by the GNRS mapping owner and shared by the mapping owner and all relevant GNRS servers.
• Policy example
  – The policy only allows a user to enter $S_3$ from $S_0$, but not from the paths $S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3$ or $S_0 \rightarrow S_1 \rightarrow S_2$.

  – **Token reuse attack**: the attacker uses a valid token (correspond to current state $S_0$) obtained previously to enter $S_3$.
    - Assume $TK_0$, $TK_1$ and $TK_2$ correspond to current states $S_0$, $S_1$ and $S_2$ respectively.
    - The attacker transited from $S_0$ to $S_1$ and therefore holds $TK_0$ and $TK_1$. Then it hides $TK_1$ and uses $TK_0$ to enter $S_3$ from $S_1$. 

\[ S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3 \]
**Spatio-temporal Token Discussion**

- **Policy examples**
  - Solution to the token reuse attack
    - Keep track of a user’s state by maintaining a token log.
    - For efficiency, the log only contains the token sequence number.
    - The GNRS server who renews or issues a token informs other GNRS servers who hold the involved mapping.
Conclusion

- We deploy access control mechanisms at a name resolution service so as to regulate access to network address information.
- Introduce spatio-temporal verification to ensure the correctness of spatio-temporal information.
- Develop a secure process for general spatio-temporal access control scenario.
- Propose a token approach to solve state transition in spatio-temporal access control.
- Present advanced functionalities and policies that the token approach can support.