CS590U

Access Control: Theory and Practice

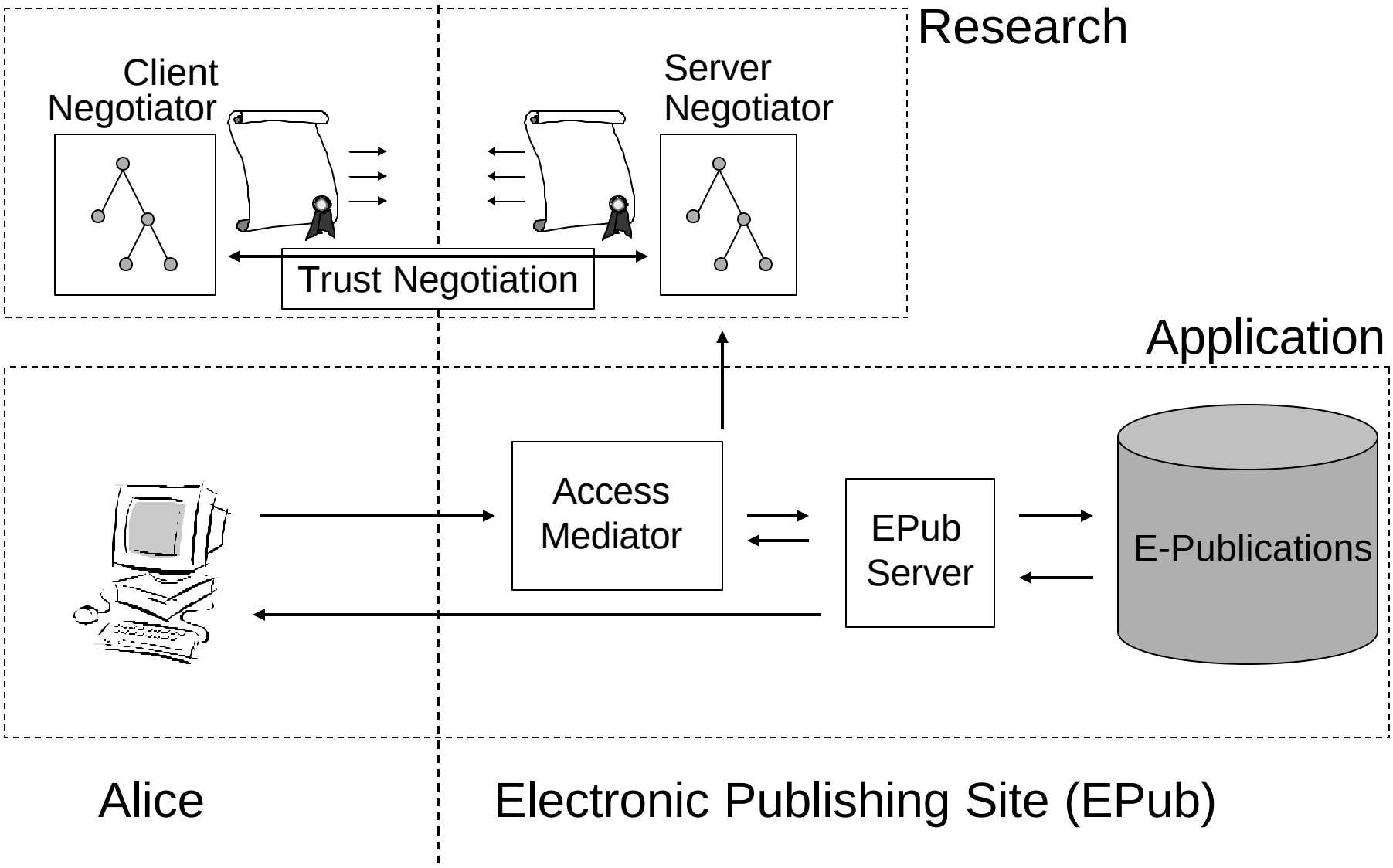
Lecture 22 (March 24)

Automated Trust Negotiation

Automated Trust Negotiation (ATN)

- Goal of ATN
  - Provide information about sensitive attributes only to authorized entities
- Approach
  - Credentials are potentially protected resources
  - Bilateral exchange of attribute credentials
  - Establish mutual trust incrementally
- What is it?
  - interactive deduction w/ additional constraints

System Design



See demos

- http://isrl.cs.byu.edu/Demos.html

Eager Strategy

- Negotiators take turns sending all unlocked credentials
  - If policy governing requested resource is satisfied, negotiation succeeds
  - Else, when no more credentials flow, negotiation fails
- Results: Completeness, Privacy (Correctness), Efficiency
- [Winsborough, Seamons, and Jones. DISCEX 2000]

Parsimoneous Strategy

- Negotiation has two phases: credential request exchange; credential exchange
- First credential request is response to original resource request
- Each subsequent request is derived from its predecessor so that satisfying it is necessary and sufficient to ensure that the predecessor can be satisfied
- If success is possible, a linear number of request exchanges leads to a request for unprotected credentials
  - Second phase begins
  - Credentials are exchanged satisfying requests in reverse order
- Results: Completeness, Privacy, Efficiency

Subsequent ATN Work

- Prunes: a quadratic backtracking strategy
  - Yu, Ma, and Winslett. "PRUNES: an efficient and complete strategy for automated trust negotiation over the Internet". CCS 2000.
- Policy graphs: protecting policy content as a sensitive resource
  - Seamons, Winslett & Yu: "Limiting the Disclosure of Access Control Policies During Automated Trust Negotiation", NDSS'01
- Interoperable strategies: closed strategy families
  - Yu, Winslett & Seamons: "Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation". *TISSEC* 2003. Conference version in CCS'01.

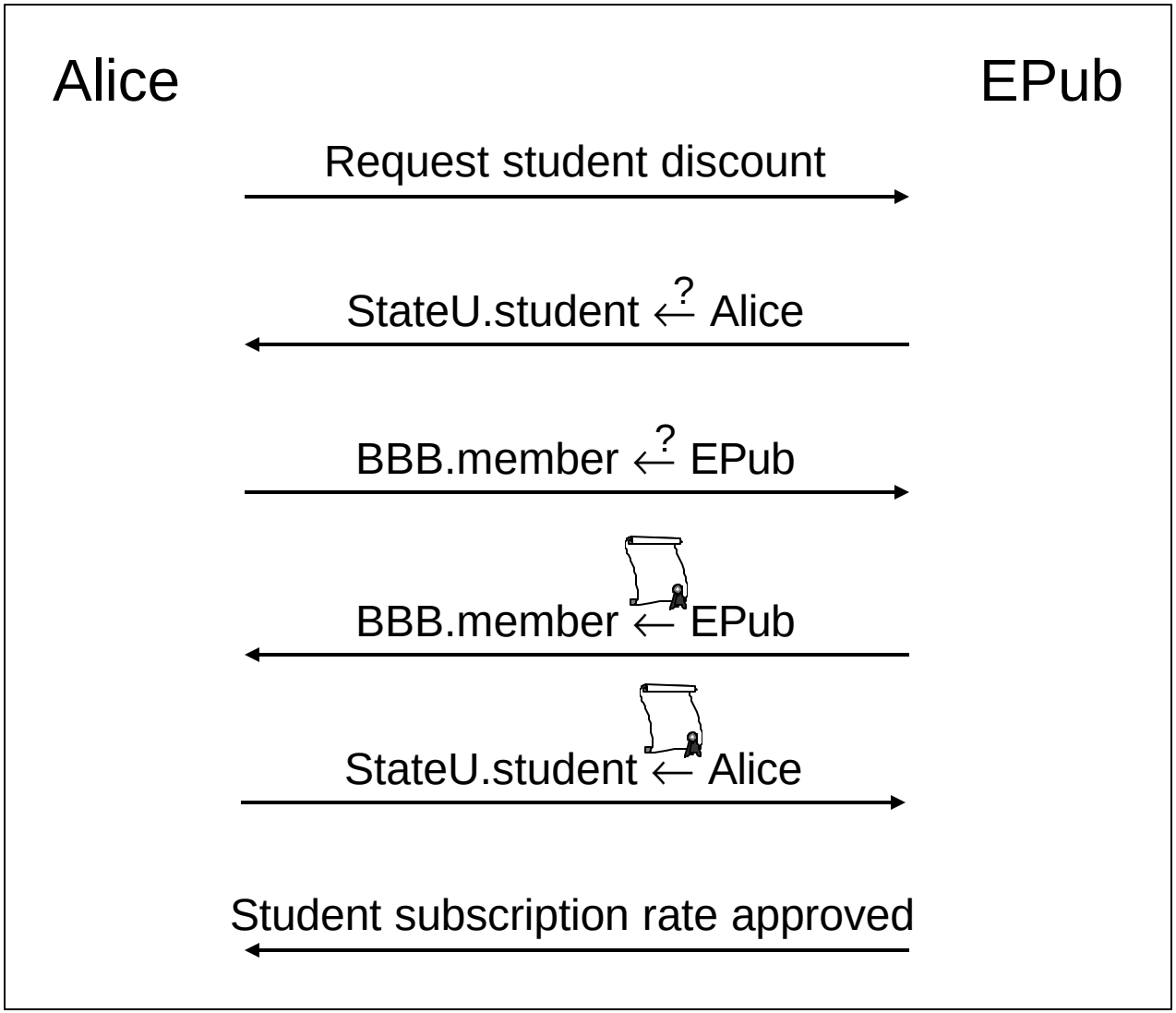
Subsequent ATN Work

- Trust Target Graph (TTG): Integrating trust management, credential discovery, privacy for sensitive attributes into ATN
  - Winsborough and Li. “Towards Practical Automated Trust Negotiation”. Policy 2002.
  - Winsborough and Li. “Protecting Sensitive Attributes in Automated Trust Negotiation” WPES 2002.
- UniPro: protecting policy content
  - Yu and Winslett: “A Unified Scheme for Resource Protection in Automated Trust Negotiation” Oakland 2003.
- A theory for safe ATN
  - Winsborough & Li: “Safety in Automated Trust Negotiation”, Oakland 2004.

More subsequent ATN work

- Bonatti & Samarati
  - “A Uniform Framework for Regulating Service Access and Information Release on the Web”, JCS 2002.
- Bertino, Ferrari & Squicciarini:
  - “Trust-\chi: A Peer-to-Peer Framework for Trust Establishment”, TKDE 2004.

Example Automated Trust Negotiation



Motivations for TTG Work

- Support a trust management policy language suited to collaborative environments and open systems
- Discover distributed credential chains
- Protect sensitive attribute information
  - Protocols, procedures, and strategies for ATN
  - Information-flow control results

Role-based Trust Management (*RT*)

- A family of credential / policy languages
  - Simplest, RT_0, satisfies these requirements
- RT_0 example: ReliefNet
  - MedixFund.purchasingA $\leftarrow$ Alice
  - ReliefNet.member $\leftarrow$ MedixFund
  - MedSup.cPartner $\leftarrow$ ReliefNet.member
  - MedSup.discount $\leftarrow$ MedSup.cPartner.purchasingA

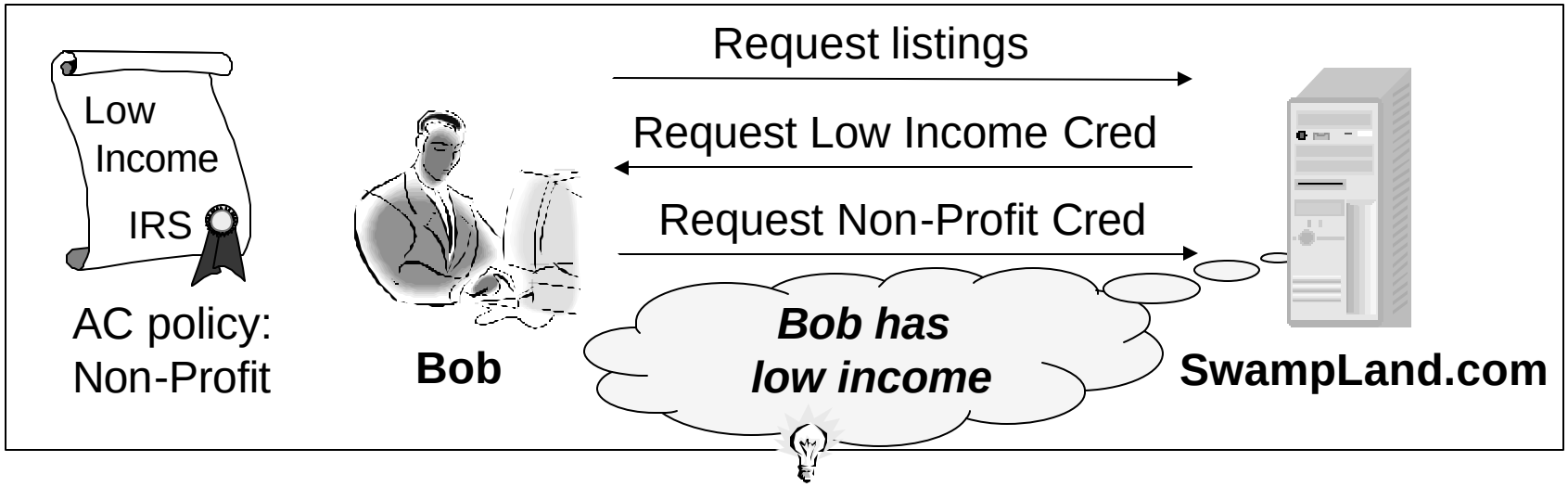
Implications for ATN (Outline)

- Negotiators must discover and collect distributed credential chains
- The potential for inference of attributes makes protection of attributes tricky

Protecting Sensitive Credentials

- Prior notion of Safety is inadequate:
  - “A credential’s access control (AC) policy must be satisfied before the credential is disclosed”
  - What does “disclose” mean?
- Most prior ATN strategies do not adequately protect information in credentials
  - Negotiator’s behavior depends on the credentials he has, no matter who he is negotiating with
  - Arises in strategies that share policy information in an effort to avoid unnecessary credential flow

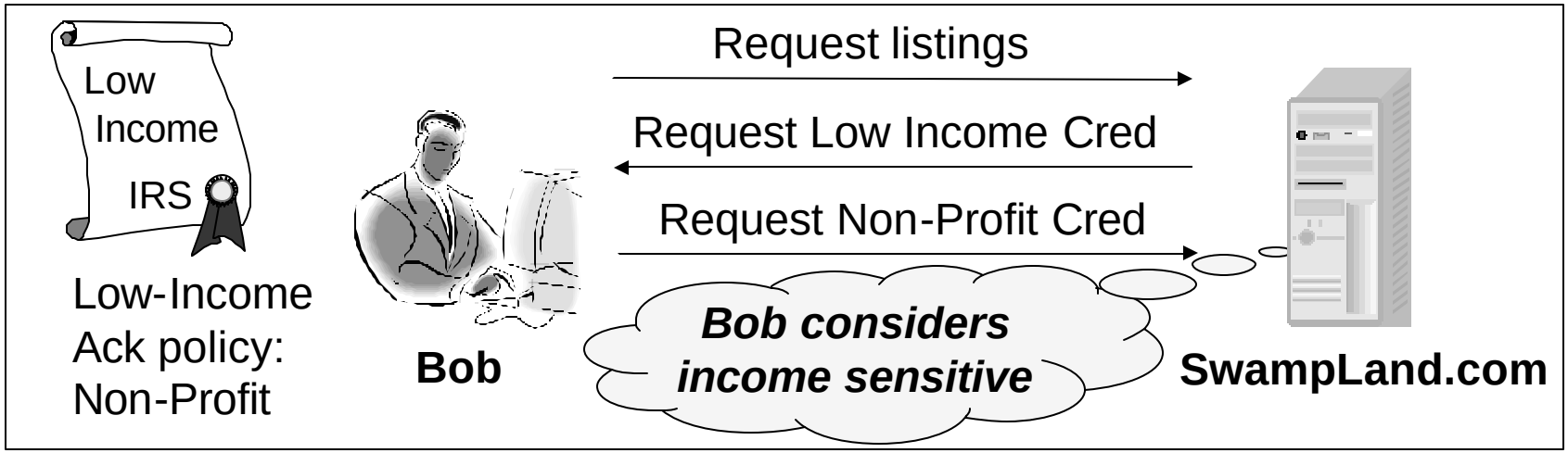
AC Provides Inadequate Safety

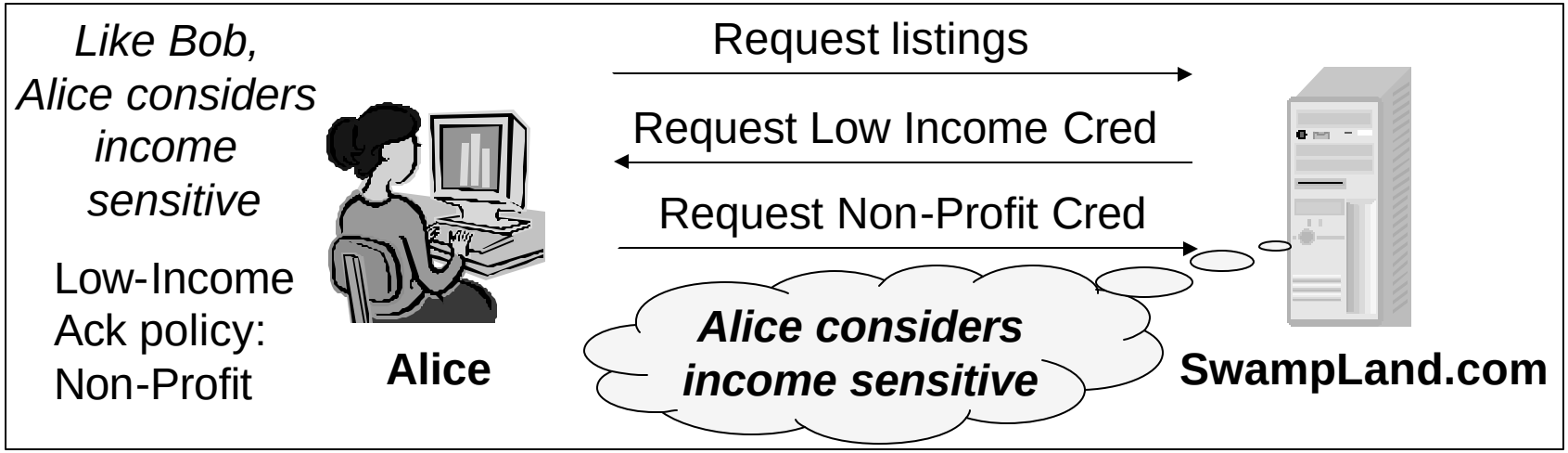


How to Safely Guide Disclosures?

- AC policies are associated with credentials
- Introduce acknowledgement (ack) policies
  - Negotiator can associate an ack policy with an attribute, whether or not he has the attribute
  - If one satisfies an attribute's ack policy, one is authorized to know whether the negotiator has the attribute
  - By providing an ack policy, a negotiator indicates only that the attribute is sensitive

Ack Policy for all Sensitive Attributes





- See TTG example from Will’s slides

Cryptographic Protocols for ATN

- Using credentials/attribute values in an oblivious way
  - Balfanz et al.: “Secret Handshakes from Pairing-Based Key Agreements”, Oakland 2003.
  - Li, Du, Boneh: “Oblivious Signature-Based Envelope”, PODC 2003.
  - Holt, Bradshaw, Seamons, and Orman. “Hidden Credentials” *WPES, 2003.*

More Cryptographic Protocols for ATN

- Hiding Policies
  - Bradshaw, Holt, & Seamons: Concealing Complex Policies with Hidden Credentials. CCS 2004.
  - Frikken, Atallah, & Li: Hidden Access Control Policies with Hidden Credentials. WPES 2004.

Open Problems

- Denial of Service attacks on ATN

Next Lecture

- Capability-based Operating Systems