Simultaneously Supporting Privacy and Auditing in Cloud Computing Systems

TYRONE GRANDISON[*], SEAN THORPE[+], LEON STENNETH[#]

[*]Proficiency Labs Intl, Ashland, Oregon, USA.
[+]School of Computing and Information Technology, University of Technology, Kingston, Jamaica.
[#]Department of Computer Science, University of Illinois, Chicago, Illinois, USA.

Talk Overview

- Motivation
- Guiding Principles
- Cloud System Operation
- Architectural and Design Foundations
- Fundamental Concepts & Constructs
- Our Proposal
- Proposal Concerns

Motivation

- Auditing of Cloud Systems gaining in importance.
  - A lot of sensitive and valuable processes, business functions and data moving into the cloud
  - Auditing enables identification of threats/risks and speeds up time to response.
- Cloud users want security and privacy protections.
  - Heightened awareness of cloud failures due to system problems and hacking.

Goals

- Creating Privacy-Preserving Logs
  - Assumes that the cloud user does not have full confidence in the cloud provider or their affiliated ecosystem.
- Enabling Auditing in a Privacy-Preserving Manner
  - Assumes there is not complete trust in the auditor and the service provider.

Guiding Principles (for building A&P controls)

- Seamless:
  - Integrate into the current mode of operation with minimal to no significant.
- Transparent:
  - It should be clear to the cloud service user what the purpose of the mechanism is and when it is functioning.
- Elastic:
  - Be able to scale to dynamically handle the request loads placed on the cloud service provider.
- Low Impact:
  - Inclusion of the mechanism should have a minor impact on the storage and performance of the cloud environment.
- Verifiable:
  - An independent third party should prove the veracity of the actions of the mechanism.

Cloud System Operation

- Cloud Use
  - User acquires access credentials, which normally includes an access key ID, and a secret access key.
  - User utilizes his ID to make a call to the API of the cloud service provider.
- User Log Generation
  - User activity leads to cloud server audit logs being generated, where the identity of the user is normally not protected.
- Auditing
  - Auditor may be internal, i.e. from the cloud user or the cloud provider, or may be an independent third party.
  - Auditor is tasked with examining cloud service controls with the intent to divine a legal opinion.
  - Audits are performed with the intent to verify conformance to standards through the review of objective evidence.

Architectural and Design Foundations

- The Mechanism Injection Point (MIP)
  - The mechanism injection point refers to the location of the A&P controls. This is the location where enforcement of the auditing and privacy rules will be performed and the supplementary mechanisms, such as data structures are situated.
- The Nature of the Cloud Service Employed
  - Cloud Model being used, i.e. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), etc.
- The Transaction Attack Vector
  - The transaction attack vector refers to the class of transactions that are evaluated in the process of assessing a possible threat.
  - There are two types of transaction attack vectors: Requests and Consequences.
- The Threat Determination Point
  - The threat determination point refers to the location where the analysis of the recorded privacy and audit events occurs, i.e. the location where breach detection and notification happens.

Fundamental Concepts & Constructs (1/3)

- Privacy - the claim of individuals, groups, or institutions to determine for themselves when, and to what extent, information about them is communicated to others
  - Privacy is the exercising of control over the disclosure and use of data
  - Data are protected from unintended eyes and from being used for unsanctioned purposes.

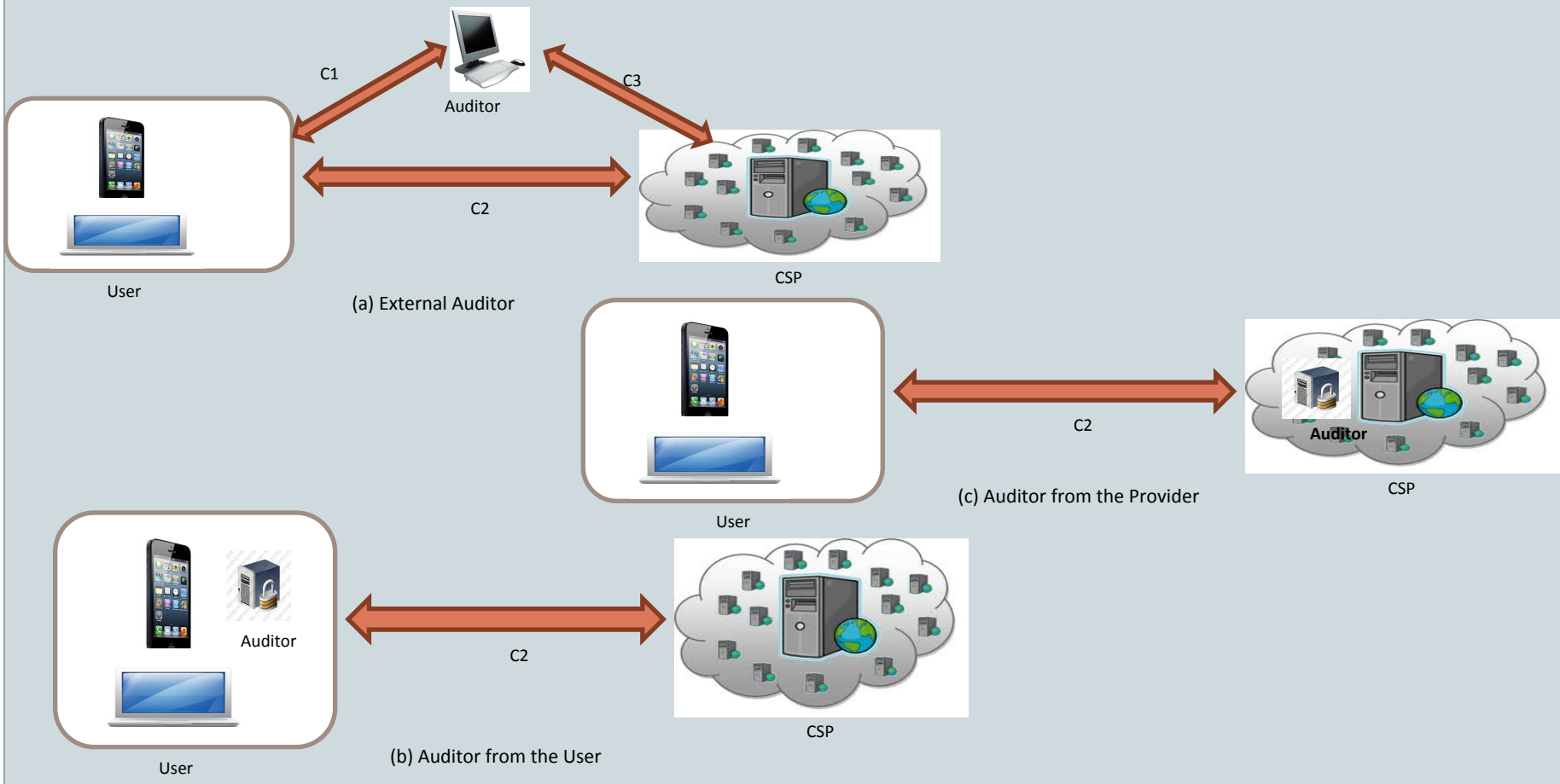
- Auditing - the systematic process of objectively obtaining and evaluating evidence regarding assertions about actions and events to ascertain the degree of correspondence between those assertions and established fact and communicating the results to interested users.
  - Auditing is about (metadata) collection (into audit logs), data extraction (of said logs), data analysis in the context of some standard (e.g. law or interesting activity, such as a security breach), and results generation and dissemination.

Fundamental Concepts & Constructs (2/3)

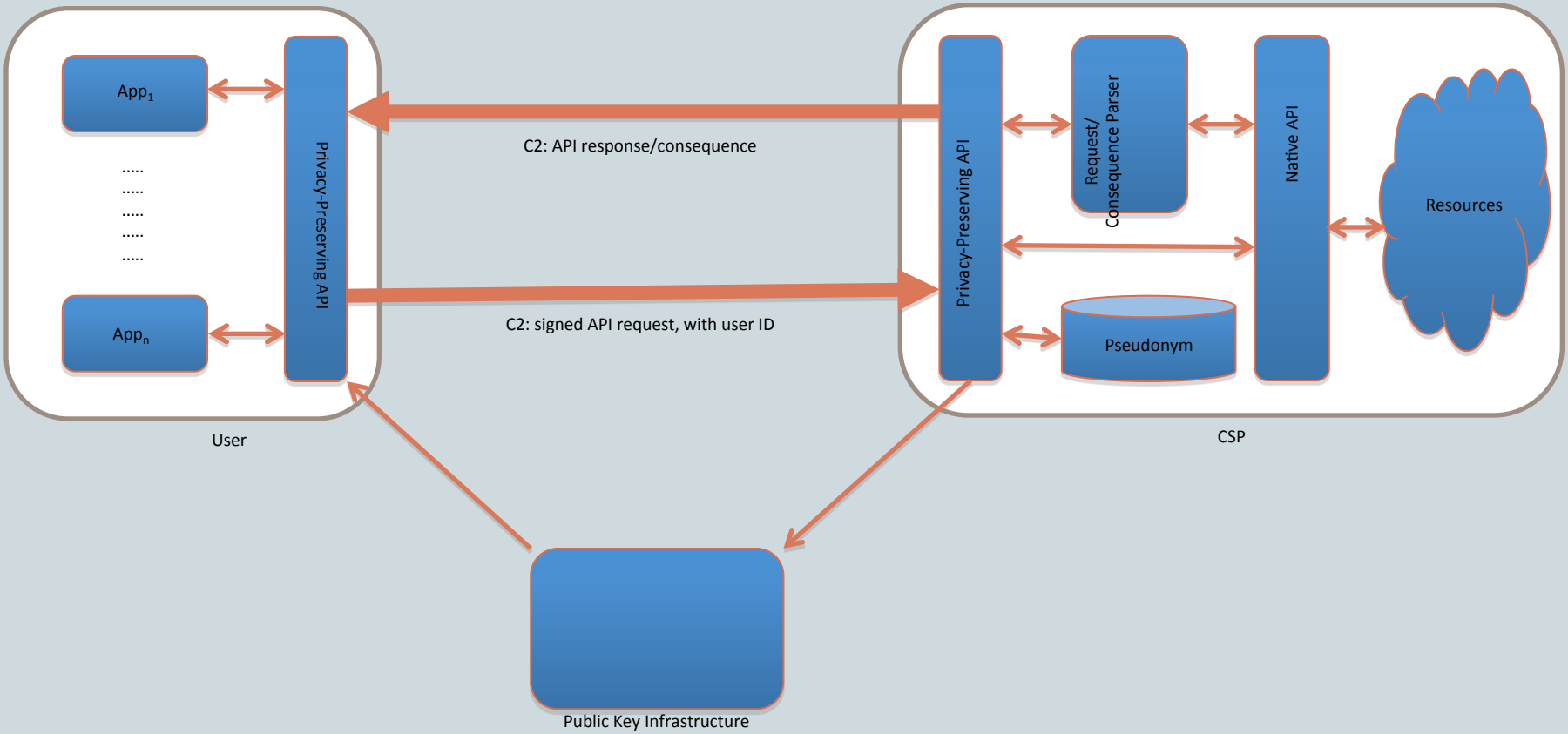
- The Current Privacy Strategy
  - Construct and deploy a methodology that allows an individual's data to be hidden in a much larger crowd of larger
  - Build and deliver a solution that securely and directly transforms individual data items to their alternate representations or surrogates.
- The Current Auditing Strategy
  - Cloud Auditing is relatively new with no established standards.
  - Techniques are being adapted from typical IT audit processes.
  - Digital forensics investigations being applied to clouds.

Fundamental Concepts & Constructs (3/3)

- The Current Threat Models



Our Proposal: Privacy-Preserving Logs



Our Proposal: Auditing in Private Mode

- User: Sends a signed request with ID to the CSP for P_A
- User: Sends a request to the auditor using P_A
- Auditor: Sends request for logs related to P_A
- CSP: Queries PKI to acquire A's public key, key_A
- CSP: Transforms audit request by encrypting sensitive parameters
- CSP: Retrieves logs related to P_A and sends it to Auditor
- Auditor: Analyzes logs with encrypted sensitive data
- Auditor: Disseminates results

Proposal Concerns

- The issue of how much data the user should reveal to the auditor for auditing to be possible is a research issue.
- In a special case where the CSP provides functionality for spatial and temporal data, cloaking techniques may be considered.
- The first step in conducting an audit (and in collecting evidence for a forensics investigation) is the process of deciphering and understanding the interactions between the cloud entities.
  - These cloud actor interactions and the linear dependencies between them provide an indicative trail of potential evidence that can be collected
  - Analysis of these interactions, based on fuzzy logs, is an area that requires further work.

Conclusion

- We provide guidelines to help in building auditing and privacy controls
  - To ensure their sustained use and relevance in these ubiquitous environments.
- We highlight the current state of affairs
- We present the foundational concepts and constructs
- We propose an approach that has the potential for future investigation and collaboration.