CS259: Security Analysis of Network Protocols
Winter 2008

Project Presentations 1

BitTorrent

Nathan Marz

Raylene Yung

BitTorrent protocol

- File split into equal-sized segments called “pieces”
- Tracker: server that keeps track of agents involved in file sharing
- .torrent file contains:
  - hash value of each piece
  - location of tracker
- Key mechanism: Download random pieces from other agents known by tracker

Security Properties

- Integrity: An attacker cannot cause

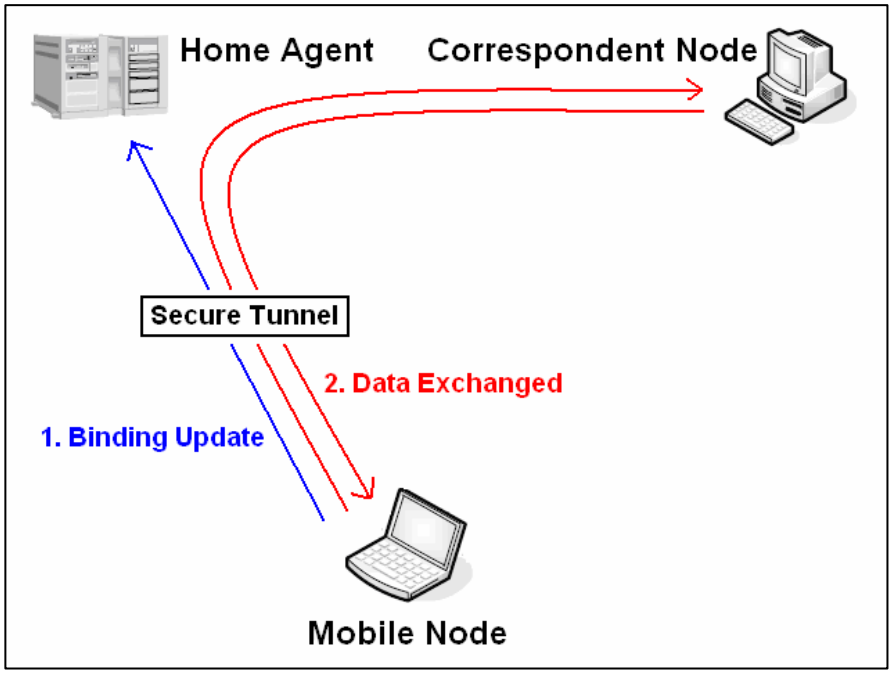
  an agent to download and accept data not equal to the original data used to create .torrent file
  - Intuition: Hashes in .torrent file can verify downloaded pieces
- Denial of Service: An attacker cannot “easily” cause an honest agent to be unable to finish a download.
  - Intuition: “Tit-for-tat” algorithms cause agents to be ignored if they don’t contribute to the torrent swarm.

Mobile IPv6 Binding Update

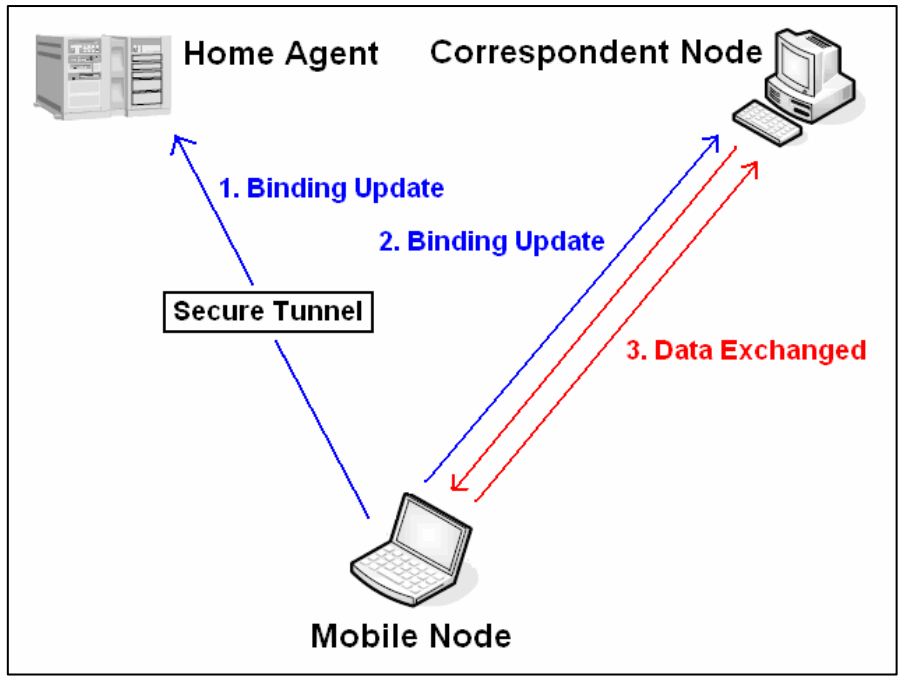
Andre Encarnacao, Greg Bayer

Mobile IPv6 Binding Update

Indirect/Triangular Routing



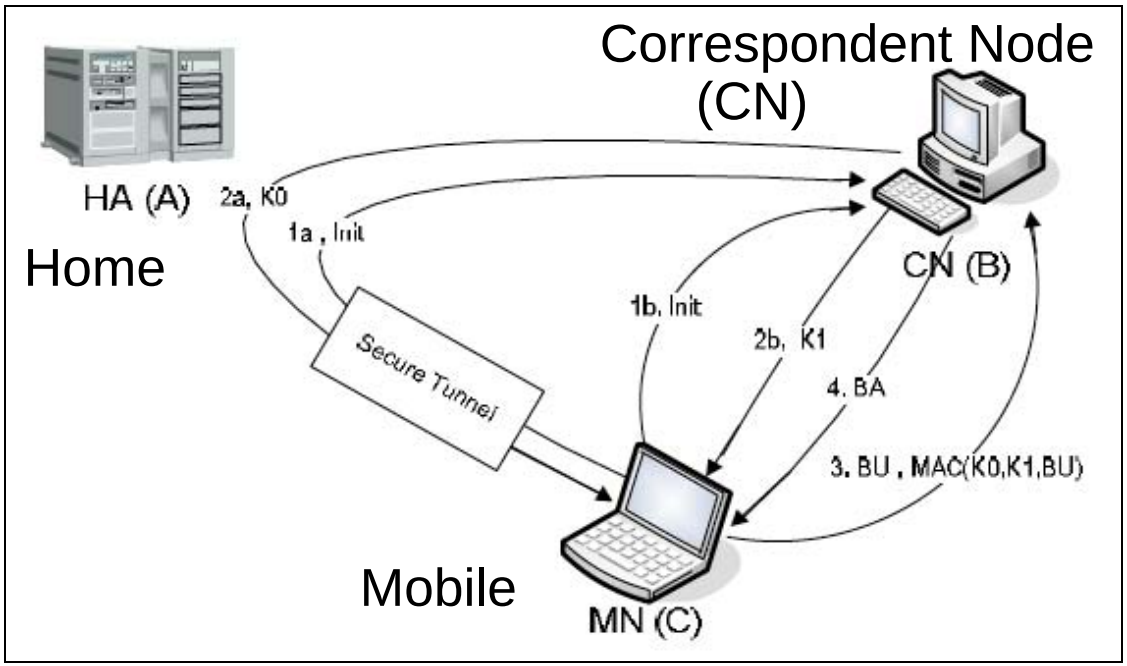
Direct Routing (Route Optimization)



- Mobile IPv4 didn't specify the direct routing optimization
- Direct routing requires a binding update over a non-secure channel
- Need a method to protect the authenticity and integrity of the binding update sent from Mobile node to Correspondent node
  - Return Routability procedure/protocol

Andre Encarnacao, Greg Bayer

Return Routability Procedure



Source: Ahmed, et al, 2007

CN ↔ Mobile via Home

1a: Home Test Init

2a: Home Test (token1)

CN ↔ Mobile

1b: Care-of Test Init

2b: Care-of Test (token2)

Kbm = SHA(token1|token2)

3: Binding Update (MAC_{Kbm})

4: Binding ACK (MAC_{Kbm})

- Authentication without Public Key infrastructure or pre-shared keys
  - Two tokens, two paths: must have both to complete update
  - Difficult for attacker to intercept both tokens & generate valid MAC
  - MAC also protects integrity of plaintext message
- Goal: Should be as secure as regular IPv4 (without mobility)
- Unusual / limited intruder model

DomainKeys Identified Mail

Chris Brigham

Tom Wang

DomainKeys Identified Mail

- Protocol for signing and verifying the originating domain for a message in transit
- Prevents domain-level forgery
- Helps deal with spam and phishing
  - Increase effectiveness of blacklists
  - Ensure the identity of an sender domain
- Backwards compatible
  - Works with all existing MTAs and MUAs

DomainKeys Identified Mail

- Example Signature Header

  DKIM-Signature: v=1; a=rsa-sha256;
  c=simple/simple; d=example.net; s=mail;
  t=1172780279;
  bh=asd123fbodyhashfoobar=;
  h=Message-
  Id:Date:To:From:Subject:Content-Type;
  b=Rsdf43sdfbase64signatureDataklsdfk=

- Public key retrieved from

DomainKeys Identified Mail

- RFC mentioned attacks
  - Misuse of body length limits
  - Misappropriated private keys
  - Key server DOS
  - DNS attacks
  - Replay attacks
  - Key revocation granularity
  - Verifier DOS
    - Malformed key, header-fields
    - RSA attack

Bluetooth Security

John Jersin

Jonathan Wheeler

Motivation for Bluetooth Study

- Increasing numbers of bluetooth devices; increasingly important data.
- IDC: there will be over 922 million Bluetooth enabled devices worldwide by 2008.
- Choice between Bluetooth and WiFi?

Known Bluetooth Attacks

- Some well known attacks when the protocol is misused.
- E.g. Using pin 0000 *and* staying in discoverable mode.
- Also, social engineering, impl errors.
- No logical errors in the protocol.

Bluetooth Security Overview

- Three security modes:
  - Security Mode 1: non-secure
  - Security Mode 2: service level enforced security
  - Security Mode 3: link level enforced security
- Will focus on link level security in mode 3.
- This is controlled by the Link Managers of each device via the Link Manager Protocol (LMP).

Bluetooth LMP Protocol Overview

- Identity Establishment
  - Use pin from 1 to 16 bytes, shared out of band.
- Authentication
  - Use a device address and nonce.
- Key Establishment
  - Share nonces and combine to form a key.
- Other Features
  - Encryption can be paused or stopped.
  - Keys and links can be discarded and regenerated.
  - Hosts can switch roles.

Bluetooth Draft Diagrams

Authentication

A - Na -> B

B - K{Na, B} -> A

B - Nb -> A

A - K{Nb, A} -> B

Key Establishment

A - K{Na, A} -> B

B - K{Nb, B} -> A

Kab = (Na XOR A) XOR (Nb XOR B)

The HTML DOM & MashupOS

Ben Newman, Shivaram Lingamneni

The HTML DOM

- The DOM is a means of translating the elements of a web page into an object hierarchy, for use in an object-oriented language such as JavaScript.
- The DOM brings with it various security concerns—what scripts should be allowed to access what elements? Security and privacy implications (e.g. cookies)
- The same-origin policy provides a simple but overly restrictive answer: full permissions for scripts from the originating site, no access for all others
- On the plus side: vulnerabilities can appear only through server-side web applications that allow malicious code same-site status (e.g. cross-site scripting)

MashupOS

- Microsoft Research's proposal for a new framework for client-side web development
- New abstractions based on notions from operating systems (e.g., an analogue for "process" called "Service-Instance", resource sharing among these Service-Instances)
- A new element called the "friv", associated with a service-instance and protecting the object hierarchy of elements inside it from outside interference
- Limited cross-domain communication among Service-Instances, according to specified rules
- Does this introduce vulnerabilities? We hope to find out.

Policy-driven Compliance Verifier / Auditor

Anthony Ho, Sharada Sundaram

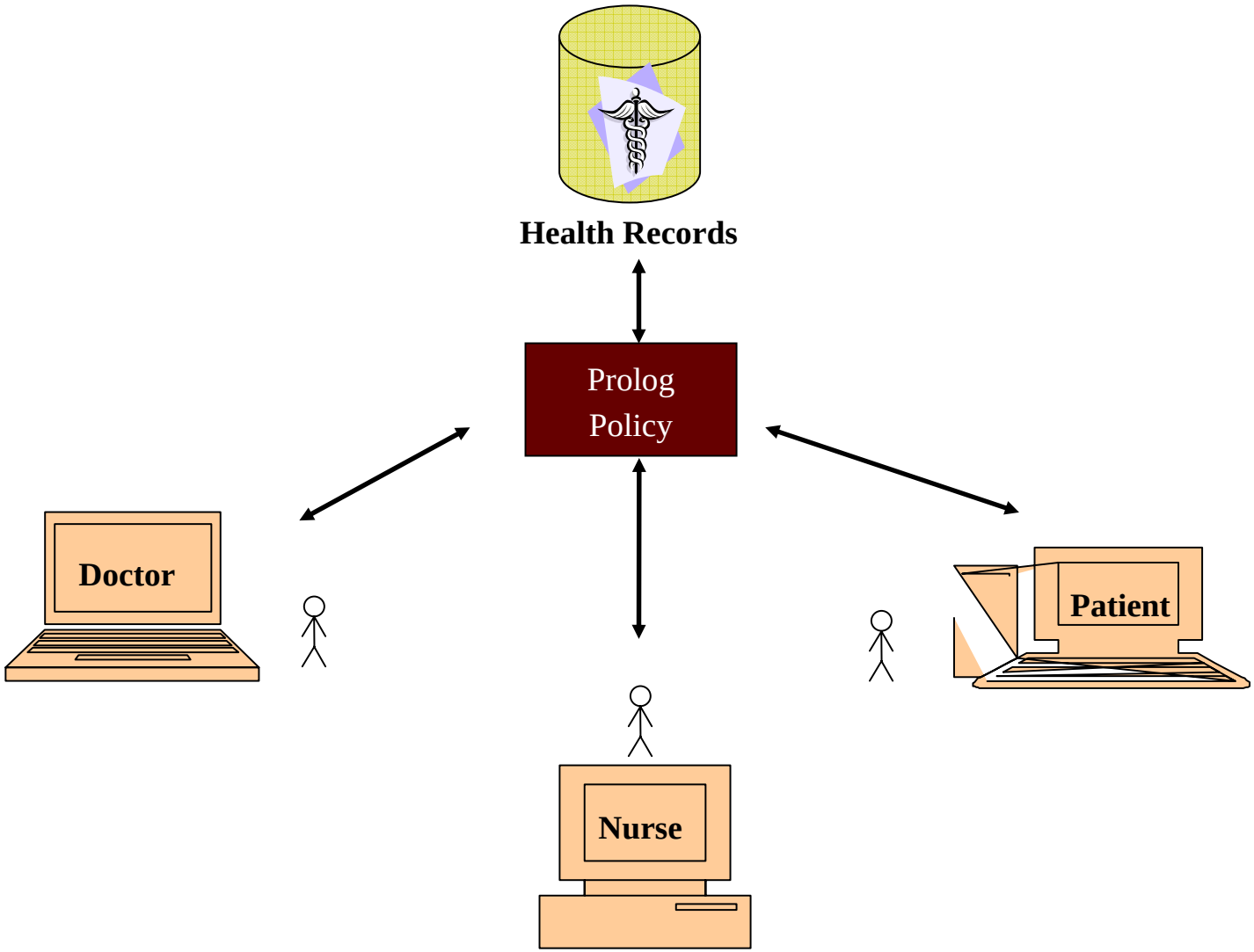
with

Adam Barth, John Mitchell, Steve Nguyen, Nicole Taheri

Background/Motivation

- The Health Insurance Portability and Accountability Act (HIPAA) is intended to protect private health care information and to create a uniform standard for dispersing personal information.
- The cost of litigation for non HIPAA compliance is high!
- HIPAA is difficult to understand.
- Difficult to tell if online systems are HIPPA compliant.

Prototype



Goals

- To express entire or major parts of HIPAA in Prolog.
- It could be run as an online auditor constantly monitoring the messages passed.
- This would be a generic template easily verifiable by lawyers, system designers, auditor and programmers.
- Consistency of HIPAA itself could be verified.

Analysis of Remote Attestation

Lavina Jain

Jayesh Vyas

Remote Attestation

What is Remote Attestation?

A method by which a host (client) authenticates it's hardware and software configuration to a remote host (server).

Mechanism and related issues:

1. Integrity measurement: On client
   - What to measure? When to measure?
   - How to securely maintain the measurements?
2. Challenge and response: Between server and client over the network
   - Server should be able to retrieve integrity measurements.
   - Server should be able to verify freshness and correctness of response.
3. Validation: On server
   - Validate that the measurement list is complete, fresh and non-tampered.
   - Determine the trust level of client.

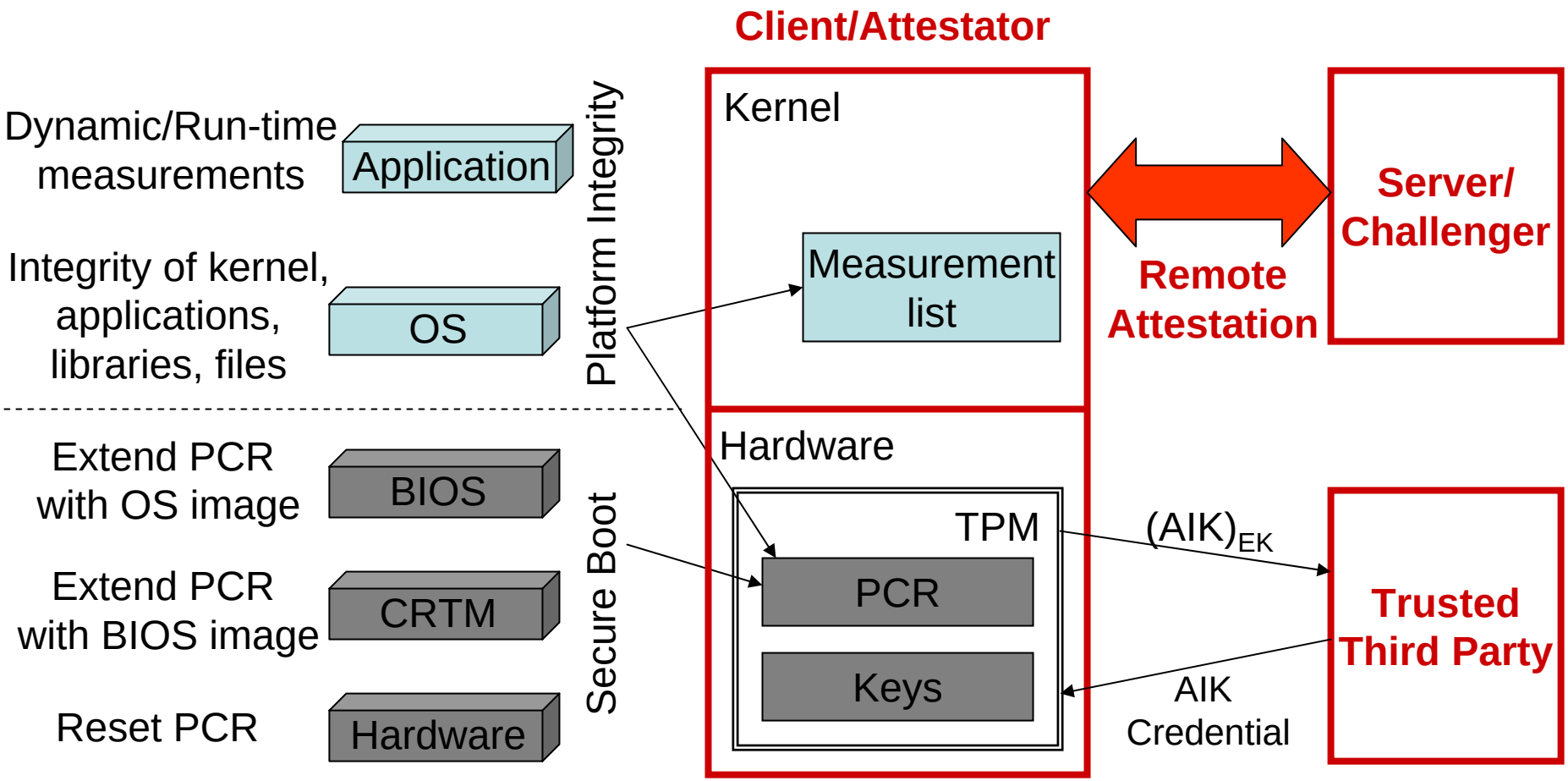
Threat:

Confidential data received from server to client may leak through malicious programs on client.

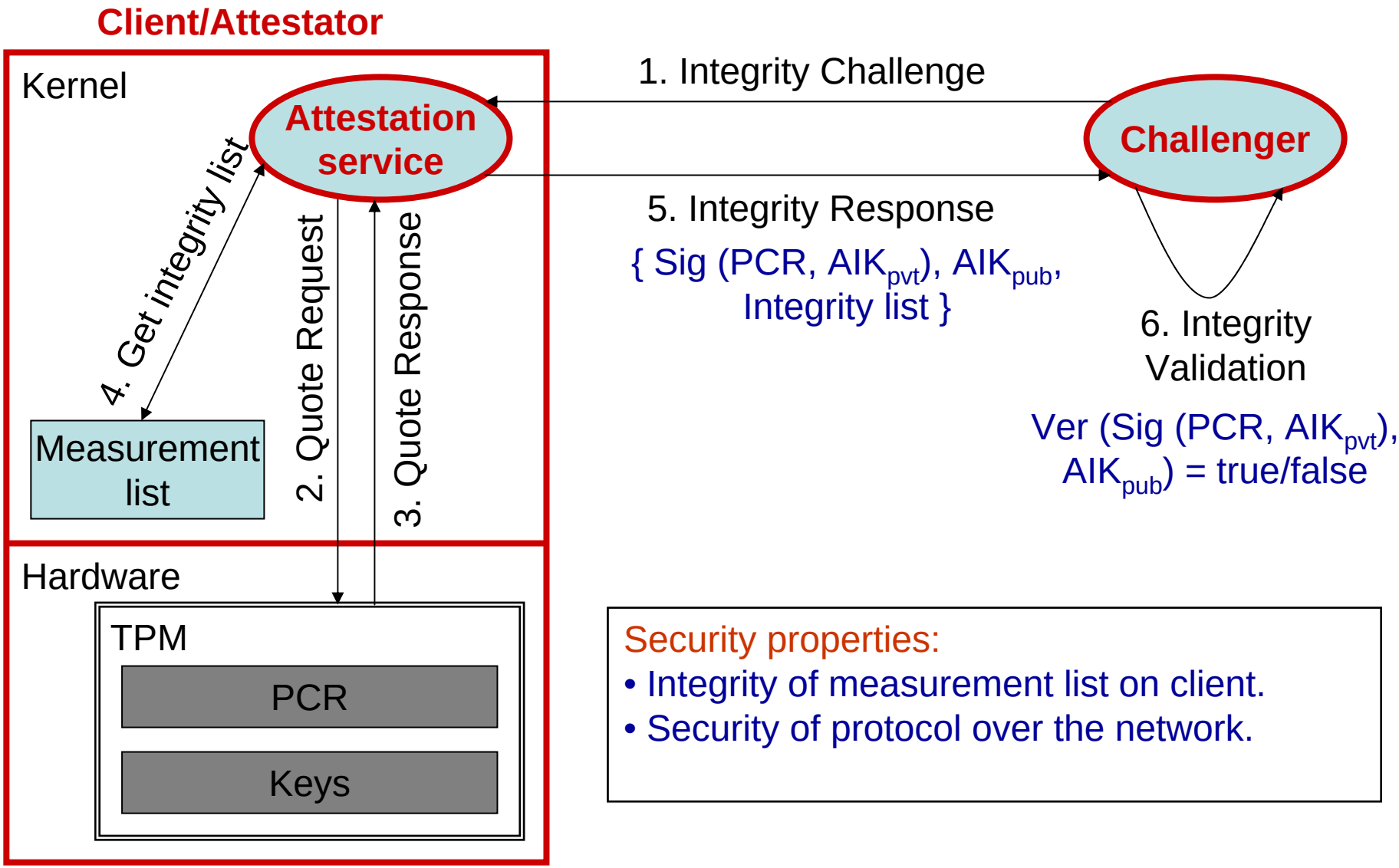
Applications:

- Establish trust upon clients accessing corporate Intranet services.
- Security against attacks on web server, browser, applications etc.

Integrity Measurement



Remote Attestation Protocol



Security properties:

- Integrity of measurement list on client.
- Security of protocol over the network.

Direct Anonymous Attestation (DAA) protocol analysis.

Sudip Regmi

Ilya Pirkin

Trusted computing.

- Trusted Computing is a future secure computer platform under development (www.trustedcomputinggroup.org)
- TPM – Trusted Platform Module – is a base component of TC:
  - is a microcontroller that stores keys, passwords and digital certificates.
  - It typically is affixed to the motherboard of a PC
  - The nature of this silicon ensures that the information stored there is made more secure from external software attack and physical theft.

Attestation problem in trusted computing.

- The user of such a platform communicates with a verifier who wants to be assured that the user indeed use an authentic TPM.
- However, the user wants her privacy protected and therefore requires that the verifier only learns that she uses a TPM but not which particular one – otherwise all her transactions would become linkable to each other.

Direct Anonymous Attestation

- A protocol which solves the attestation problem without highly available online Privacy CA (the original workgroup proposal)
- Based on the Camenisch-Lysyanskaya Signature Schema (“group signing”).
- Interactive protocol between the verifier and the host containing the TPM.

Our Focus

1. If intruder can pretend to be authentic TPM?
2. If intruder can break the anonymity of the TPM hosts?
3. If a TPM gets compromised will it break the security of other TPM and their users?
4. Is it possible to attest via a proxy and how it affects security properties?
5. We will attempt to remove some parts of the protocol or message fields (e.g nonces) and will see whether the security properties still hold.

A Probabilistic Analysis of the Pynchon Gate Personal Information Retrieval System

Fred Wulff

Pynchon Gate

- 2005 ACM WPES paper by Sassaman, Cohen, and Mathewson
- Basic need: Retrieving mail from a pseudonymous server. Problems with onion routing, sending to everybody.
- Solution: Distributed hash table. Provides information theoretical anonymity in presence of n-1 corrupt servers.

Known Attack and Possible Modeling Approaches

- Our old friends, the Byzantine generals.
- One adversary server can mount a DOS attack.
- Not found in the original paper, but fix proposed.
- Can we effectively model the probability of DOS being successful (e.g. given small number of servers) using a small number of rules?
- Other possibilities for probabilistic modelling (probably using PRISM)

802.16g-2007 (WiMAX)
(Management Plane Procedures and Services)

-Provides standards for network resource management
-Applies to both fixed and mobile WiMAX
-Large amendment (202 pgs)

Matt Bravo
mbravo@stanford.edu

Security management in the services plane

- Analyze accounting management procedure (uses key exchange and digital signatures)
- Check for information leaks in addition to protocol attacks
- Check for misbehavior on the client end to subvert accounting procedure