Стандарты в области безопасности Информационных и Телекоммуникационнных Систем

Silk Security Workshop 2004
21-24 июня, 2004

Yuri Demchenko, University of Amsterdam
<demch@science.uva.nl>

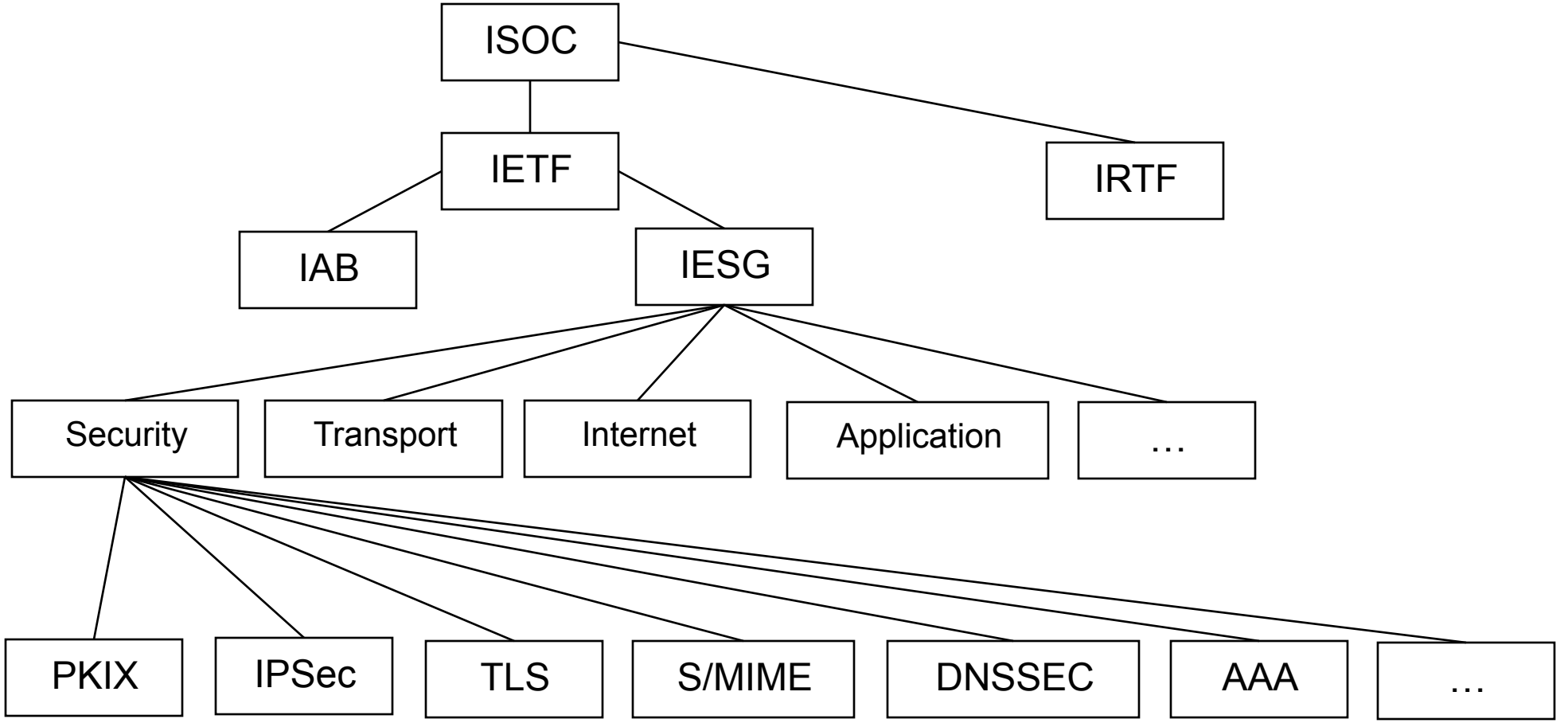
Содержание

- Организации стандартизации
- Модель Взаимодействия Открытых Систем
- Архитектура безопасности открытых систем (ISO 7498-2)
- Механизмы безопасности уровня данных группы IEEE 802
- Стандарты и механизмы безопасности Интернет
- Стандарты в области реагирования на компьютерные инциденты безопасности
- Инфраструктура открытых ключей PKI
- Технологии безопасности на основе XML
- Современные технологии аутентификации и авторизации

Организации стандартизации

- ISO/IEC, IEEE: Общие/архитектурные вопросы безопасности
  - Стандарты ISO/IEC, IEEE
- ITU (International Telecommunication Union): Стандарты безопасности телекоммуникационных систем
  - Стандарты X, V, T, H, etc.
- IETF (Internet Engineering Task Force): Стандарты безопасности Интернет (RFC)
- OASIS (Organization for the Advancement of Structured Information Standards): Стандарты безопасности на основе XML (для бизнес-приложений)
- NIST, CEN, ETSI: Национальные и региональные стандарты безопасности
- Другие специализированные консорциумы и форумы
  - GGF (Global Grid Forum) - стандарты для Грид-приложений
  - Liberty Alliance Project – Атентификация и идентификация в Интернет

Структура и направления стандартизации IETF



Рабочие группы IETF по вопросам безопасности (2004) - http://www.ietf.org/html.charters/wg-dir.html

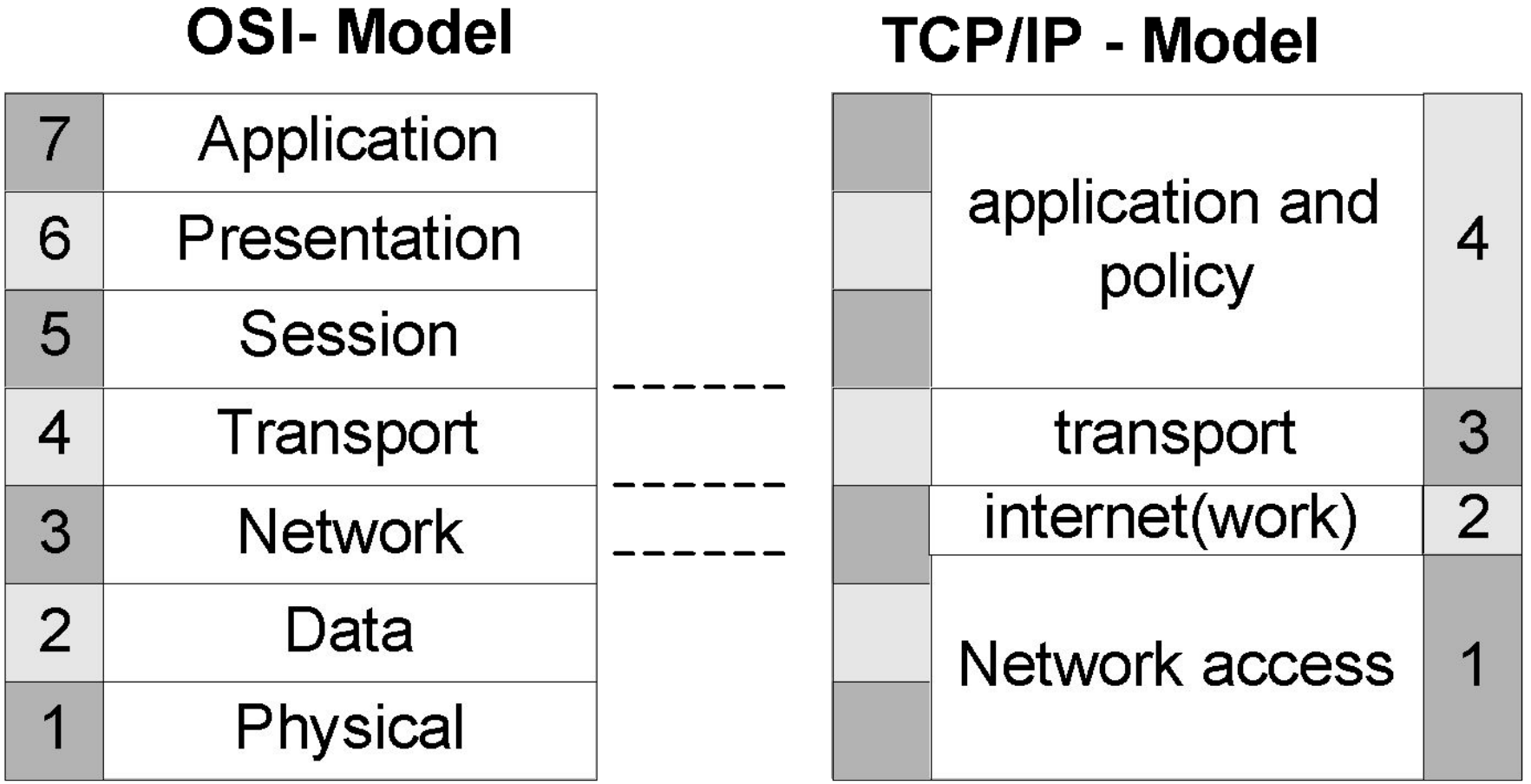
enroll, idwg, inch, ipsec, ipseckey, ipsp, kink, krbwg, ltans, mobike, msec, openpgp, pki4ipsec, pkix, sacred, sasl, secsh, smime, stime, syslog, tls, aaa

Модель Взаимодействия Открытых Систем (ВОС)
Open System Interconnection (OSI) Reference Model

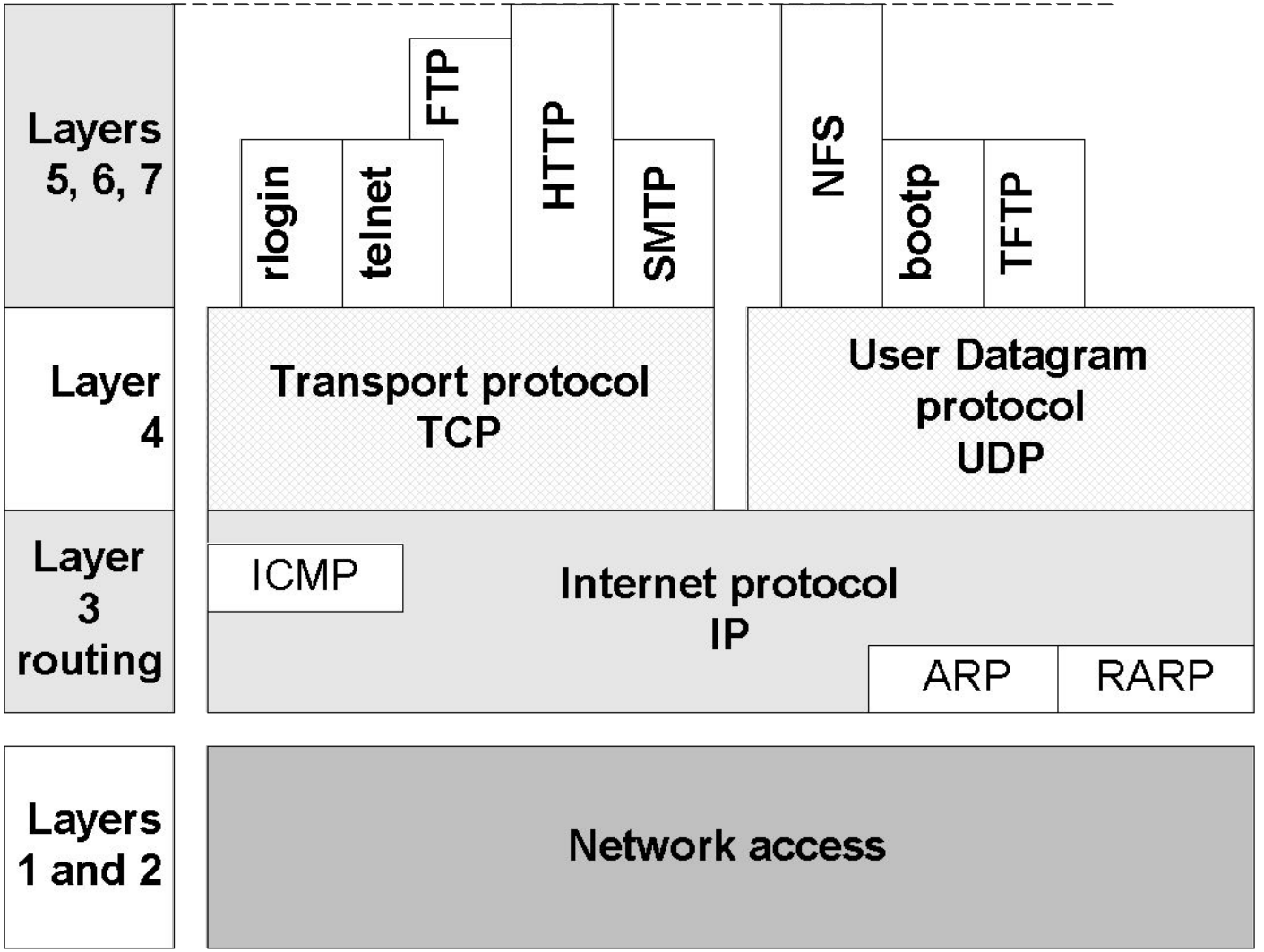
ISO 7894-1984/ITU X.200

Уровни ВОС	Реализуемые функции
Прикладной Application	Сетевые приложения такие, как передача файлов и эмуляция терминалов
Представительный Presentation	Форматирование данных и кодирование
Сеансовый Session	Установление и поддержание сеанса связи
Транспортный Transport	Обеспечение доставки между конечными точками
Сетевой Network	Даставка пакетов информации, включая маршрутизацию
Данных Data Link	Передача данных, формирование пакетов, контроль ошибок
Физический Physical	Передача двоичных данных через среду

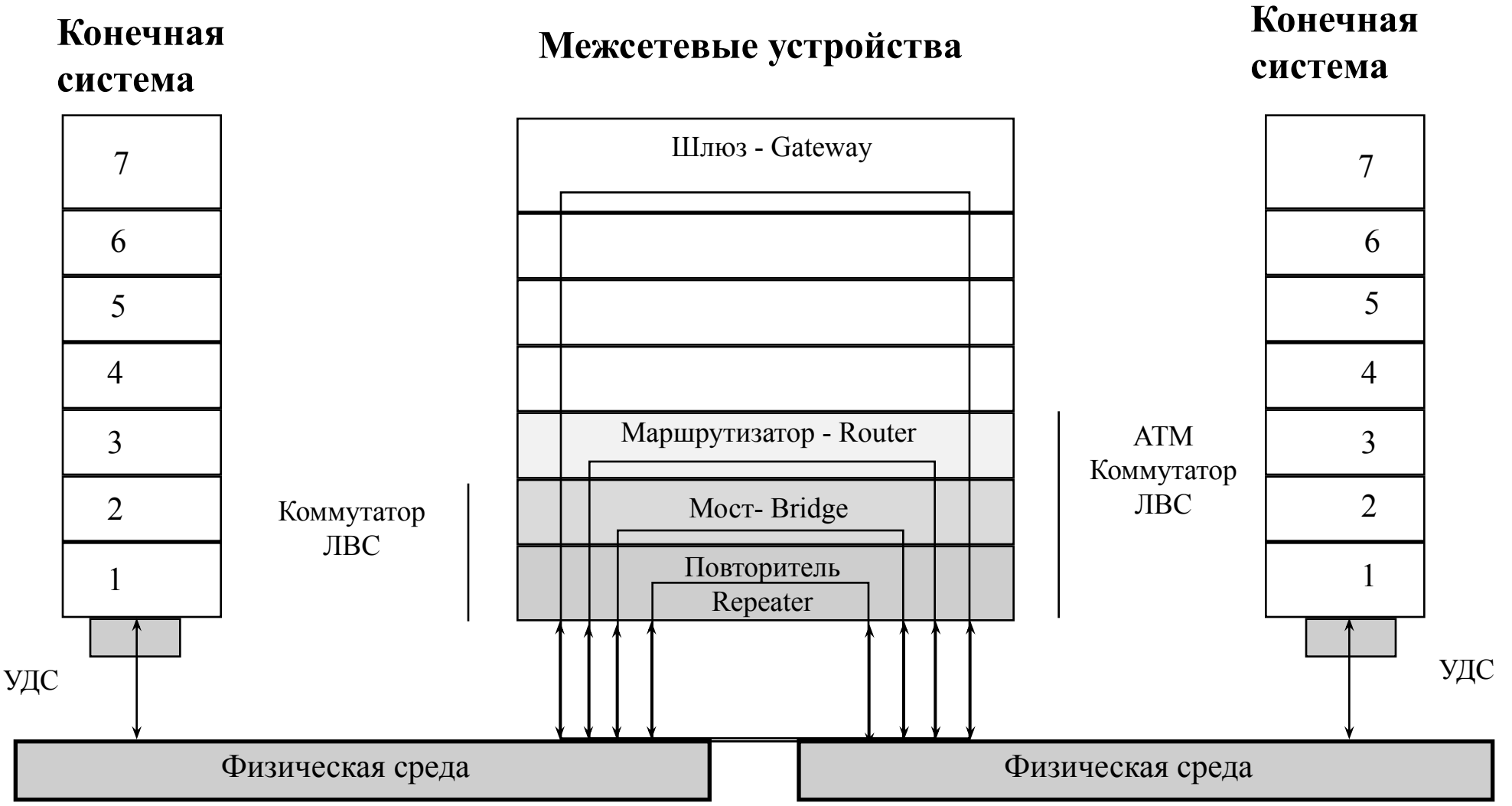
Группа протоколов TCP/IP (1)



Группа протоколов TCP/IP (2)



Основные структурные элементы сетей



Объекты защиты в ИТС

Вычислительные ресурсы и инфраструктурные компоненты

- Вычислительные системы
- Телекоммуникационные системы
- Системы управления сетью и другими обьектами
- Центральные компоненты различных сервисов, например, DNS, PKI, LDAP

Информационные ресурсы

- Интеллектуальная собственность
- Конфиденциальная информация
- Личная информация, например, о клиентах, больных
- Информация о третьих лицах, например, о партнерах или другая бизнес-информация

Безопасность и Реагирование на инциденты безопасности

- (Техническая) Безопасность представляет собой комплекс технических средств и мер, направленных на обеспечение нормальной работы системы или нормального выполнения поставленной задачи/фунции в условиях непредвиденных внешних факторов и воздействий как умышленных, так и неумышленных
  - В основном, представляет собой профилактические/проактивные меры
  - Нет и не может быть совершенной безопасности
  - Безопасность стоит денег, и риск оценивается относительно возможного ущерба

- Реагирование на инциденты безопасности является важным компонентом обеспечения безопасности, хотя является реактивной функцией
  - Обратная связь к мерам безопасности
  - Необратимость наказания
  - Восстановление потерь

Архитектурная концепция безопасности ISO 7498-2

Компоненты и принципы

- Определение сервисов и механизмов безопасности
  - Услуги – абстрактные понятия, характеризующие свойства и требования к системе
  - Механизмы – конкретные меры для реализации услуг
- Уровневая модель построения услуг безопасности
- Соотнесение услуг безопасности к уровневой модели
- Соотнесение механизмов безопасности к услугам

Принципы построения уровневой модели безопасности

- Число альтернативных способов обеспечения безопасности должно быть минимизировано
- Услуги безопасности могут работать более чем на одном уровне
- Функции безопасности не должны дублировать существующие аналогичные функции системы, а напротив, использовать их
- Применение механизмов безопасности не должно нарушать независмости уровней
- Количество неконтролируемых/доверительных функций должно быть минимизировано
- Услуги безопасности должны быть определены так, чтобы допускать модульное дополнение к основным сервисам (plugability)

Базовые сервисы безопасности ISO 7498-2

- Конфиденциальность – Confidentiality
- Аутентификация – Authentication
- Целостность – Integrity
- Контроль доступа – Access control
- Причастность («неотпирательство») – Non-repudiation
- Доступность - Availability

Общие механизмы безопасности ISO 7498-2

- Шифрование – Encryption
- Цифровая подпись – Digital signature
- Обеспечение целостности (потоков) данных – Data (stream) integrity
- Заполнение трафика – Traffic padding
- Аутентификация – Authentication
- Контроль доступа – Access control
- Нотаризация - Notarisation

Механизмы безопасности TCP/IP (IETF-1)

- **One-Time Passwords** - Одноразовый пароль
- **HMAC** (Keyed-Hashing for Message Authentication) - RFC2104
  - Механизм аутентификации сообщений на основе секретных ключей
- **IPSec** - RFC2401, RFC2402, RFC2406, RFC2407, RFC2411
  - Базовый проткол шифрования и аутентификации IP-уровня. Применяется для защиты коммуникаций host-to-host, host-to-gateway, gateway-to-gateway. Является основой для VPN (Virtual Private Network)
- **TLS** (Transport Layer Security) - RFC2246
  - Обеспечивает зашифрованный, аутентифицируемый канал, который работает поверх TCP. Серверная часть обычно аутентифицируется при помощи Сертификата открытого ключа (СОК), клиент может также иметь сертификат и осуществлять взаимную аутентификацию.
- **SASL** (Simple Authentication and Security Layer) – RFC 2222
  - Обеспечивает сервисы безопасности для протоколов на основе соединений, в частности, BEEP, IMAP, LDAP, POP, SMTP
- **GSS-API** (Generic Security Service Application Program Interface) - RFC2744
  - Программный интерфейс для обеспечения интеграции сервисов аутентификации, делегирования, защиты сообщений с базовыми сервисами в распределенных сетевых и вычислительных приложениях

Механизмы безопасности TCP/IP (2)

- **DNSSEC** - RFC2535
  - Позволяет подписывать DNS-записи, предотвращая возможность подмены ответов DNS во время транспорта. Теоретически может использоваться для распространения СОК
- **Security/Multipart (S/MIME)** – RFC1847
  - Шифрование и цифровая подпись много-компонентных сообщений электронной почты на основе PKI
- **Digital Signatures** - Цифровая подпись
- **OpenPGP** – RFC2440, RFC3156
  - Шифрование и цифровая подпись сообщений электронной почты
- **Firewalls** - Сетевые экраны как топологический механизм защиты
- **Kerberos** – RFC1510
  - Механизм взаимной аутентификации и обмена секретными ключами
- **SSH** – обесечение безопасного соединения между клиентом и сервером

Нерекомендуемые незащищенные механизмы

- Текстовый пароль - Plaintext Passwords
- Аутентификация на основе IP-адреса - Address-Based Authentication
- Аутентификация на основе доменного имени - Name-Based Authentication

Механизмы безопасности уровня данных группы IEEE 802

IEEE 802.10: расширяет архитектуру безопасности ISO 7498-2 с целью добавления сервисов безопасности Аутентификации, Контроля доступа и Целостности данных к уровням данных и сетевому

IEEE 802.1X: Определяет механизмы аутентификации с использованием сетевых портов, использует динамическое распределение сеансовых ключей для WEP-шифрования. Использует EAP для аутентификаци и обычно использует сервер RADIUS.

IEEE 802.11i: Будущий стандарт безопасности, который использует механизм аутентификации 802.1X и добавляет стандарт шифрования AES.

WPA (Wi-Fi Protected Access): механизм шифрования, который устраняет уязвимости WEP. WPA также использует механизмы аутентификации 802.1X.

EAP (Extensible authentication protocol): протокол «точка-точка», который поддерживает множественные механизмы аутентификации. Имеет реализации для множества ОС.

TKIP (Temporal key integrity protocol): используется в стандартах 802.1X и WPA для аутентификации. Устраняет проблемы WEP.

WEP (Wired equivalent privacy): протокол безопасности 802.11 для беспроводных сетей.

Remote Access Dialin User Service (RADIUS)

RADIUS широко используется для контроля доступа удаленных пользователей, включая аутентификацию, авторизацию и учет (AAA - authentication, authorization, accounting).

- RFC 2865, RFC 2869
- RADIUS определяет собственный механизм аутентификации и защиты целостности, а также обеспечения конфиденциальности определенных «скрытых параметров».
- Сервер RADIUS используется как центральный сервер аутентификации, который хранит или имеет доступ к базе данных пользователей
  - Сервер доступа запрашивает данные идентифицирующие пользователя (напр., имя, пароль) и формирует запрос к серверу RADIUS
  - RADIUS проверяет условия доступа для конкретного пользователя (как минимум, имя и пароль) и выдает положительное и отрицательное решение
    - Может запрашивать другие серверы RADIUS
  - Выполняет также функцию учета времени работы пользователя и биллинга

Authentication, Authorisation, Accounting (AAA)

- Группа стандартов, определяющих архитектуру и инфраструктуру распределенных сервисов аутентификации, авторизации и учета
  - RFC 2903 - Generic AAA Architecture
  - RFC 2904 - AAA Authorization Framework
  - RFC 2905 - AAA Authorization Application Examples
  - RFC 2906 - AAA Authorization Requirements
  - RFC 3334 - Policy based accounting
- Базовая архитектура нашла внедрение и развивается для мобильных сетевых приложений
- Дальнейшее развитие в направлении авторизации и контроля доступа на основе политики

Стандарты в области реагирования на компьютерные инциденты безопасности (1)

RFC 2196 - Site Security Handbook (на замену RFC1244)

- Руководство по составлению политики безопасности и поддерживающих методик для систем, подключенных к Интернет

RFC 2350 - Expectation for Security Incident Response Teams

- Описывает, что пользователи Интернет должны ожидать от служб реагирования на компьютерные инциденты безопасности. Предоставляет методику как организовать Центр реагирования на компьютерные инциденты безопасности (CSIRT - Computer Security Incident Response Team) и базовые документы: Политика безопасности, Политика реагирования на инциденты безопасности, и другие

RFC2505 - Users' Security Handbook

- Руководство пользователям по обеспечению безопасности информации, данных, и телекоммуникаций

RFC3013 - Recommended Internet Service Provider Security Services and Procedures

- Описывает в форме рекоммендаций, что пользователи Интернет могут ожидать (и требовать) от Интернет сервис- провайдеров

RFC3227 - Guidelines for Evidence Collection and Archiving

- Рекомендации по сбору и хранению улик и другой информации, связанной с компьютерными инцидентами безопасности

Стандарты в области реагирования на компьютерные инциденты безопасности (2)

Форматы для описания и обмена информацией о компьютерных инцидентах безопасности

- IDMEF – Intrusion Detection Message Exchange Format
- IODEF – Incident Object Description and Exchange Format
  - RFC3067 - Incident Object Description and Exchange Format (IODEF) Requirements
- Новый RID – Real-time Internetwork Defense (поддерживается US AFC)
  - Проследить источник атаки и остановить или уменьшить влияние атаки

RFC 2828 - Internet Security Glossary

- Содержит расширенный список терминов по безопасности как из области операционной и реагирования на компьютерные инциденты безопасности, так и из области технологий безопасности данных и приложений

ISO/IEC 17799-1 – Code of Practice for Information Security Management

ISO17799 – детальный документ, описывающий рекомендуемые меры и методы обеспечения безопасности и имеет следующие разделы

1. Business Continuity Planning
2. System Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organisation
8. Computer & Network Management
9. Asset Classification and Control
10. Security Policy

ISO17799 составляет основу для многих методик аудита и анализа рисков компьютерных систем.

Основы PKI

PKI (Public Key Infrastructure) – Инфраструктура открытых ключей (ИОК)

- RFC 2459, RFC 2560, RFC 3280, RFC 3647,
- Основа ИОК – Сертификат открытого ключа (СОК, PKC - Public Key Certificate) по стандарту X.509 (ITU-T)
  - Другие компоненты: CP – Certificate Policy, и CRL – Certificate Revocation List
- Связывает идентификатор (имя собственное, distinguished name) субьекта с его открытым ключом
  - PKC подписывается цифровой подписью Центра удостоверения (CA - Certification Authority)
- Компоненты ИОК
  - Identification Service (IS)
  - Registration Authority (RA)
  - Certification Authority (CA)
  - Certificate Repository (CR), normally built on LDAP

PKC vs AC: Цели

- X.509 PKC связывает идентификатор субьекта и его открытый ключ
  - PKC подписывается цифровой подписью Центра удостоверения (CA - Certification Authority)
- Сертификат Атрибутов (AC – Attribute Certificate) связывает идентификатор субьекта с его атрибутами
  - AC подписывается цифровой подписью Центра удостоверения атрибутов (AA - Attribute Authority)
- AC является компонентом X.509 Role-based PMI
  - AC не содержит открытого ключа
  - AC может содержать атрибуты, которые характеризуют принадлежность субьекта к определенной группе, его роль, уровень доступа (security clearance), или другую информацию для авторизации
- PKC используется для аутентификации, а AC – для авторизации
  - AC может содержаться в ответе сервера аутентификации
- Аналогия: PKC - как паспорт, а AC – как виза

PKC vs AC: Certificates structure

X.509 PKC

- Version
- Serial number
- Signature
- Issuer
- Validity
- **Subject**
- **Subject Public key info**
- Issuer unique identifier
- Extensions

X.509 AC

- Version
- **Holder**
- Issuer
- Signature
- Serial number
- Validity
- **Attributes**
- Issuer unique ID
- Extensions

X.509 PKC Fields and Extensions – RFC 3280

X.509 PKC Fields

- Serial Number
- **Subject**
- **Subject Public Key**
- Issuer Unique ID
- Subject Unique ID

X.509 PKC Fields

- Private Extensions
  - Authority Information Access
  - Subject Information Access
- Custom Extensions

X.509 PKC Extensions

- Standard Extensions
  - Authority Key Identifier
  - Subject Key Identifier
  - **Key Usage**
  - Extended Key Usage
  - **CRL Distribution List**
  - Private Key Usage Period
  - **Certificate Policies**
  - Policy Mappings
  - Subject Alternative Name
  - Issuer Alternative Name
  - Subject Directory Attributes
  - Basic Constraints
  - Name Constraints

AC Attribute Types and AC Extensions

AC Attribute Types

- Service Authentication Information
- Access Identity
- Charging Identity
- **Group**
- **Role**
- Clearance
- Profile of AC

AC Extensions

- Audit Identity
- To protect privacy and provide anonymity
- May be traceable via AC issuer
- AC Targeting
- Authority Key Identifier
- Authority Information Access
- CRL Distribution Points

Безопасность приложений на основе XML и традиционная модель сетевой безопасности

Традиционная модель сетевой безопасности (ISO7498-2):

- Host-to-host или point-to-point безопасность
- Ориентированная на архитектуру клиент/сервер
- Ориентированные на коммуникации с соединением (connection-oriented) или без соединения (connectionless)
- В общем случае единый доверительный домен (на основе PKI)

Безопасность приложений на основе XML

- Безопасность между конечными точками или приложениями (end-to-end)
- Ориентированна на документ (или семантический обьект)
  - Мандаты и маркеры безопасности могут быть ассоциированы с документом или сообщением или их частью
- Существующие технологии WS-Security обеспечивают безопасность между разными административными доменами и доменами безопасности
- Позволяет создавать динамические и виртуальные ассоциации безопасности

Компоненты безопасности XML - приложений

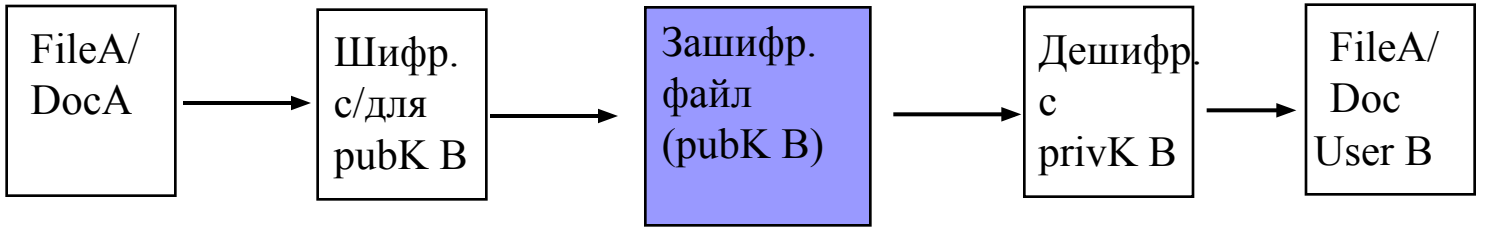
- XML Signature
- XML Encryption
- Декларации безопасности (Security Assertions)
  - SAML (Security Assertion Mark-up Language)
  - XACML (XML Access Control Mark-up Language)
- XKMS (XML Key Management Specification)
- Архитектурные расширения
  - Web Services Security (WS-Security)
  - OGSA Security

Основные черты XML-подписи

Фундаментальная черта: возможность подписывать отдельные части документа так же как и целый документ.

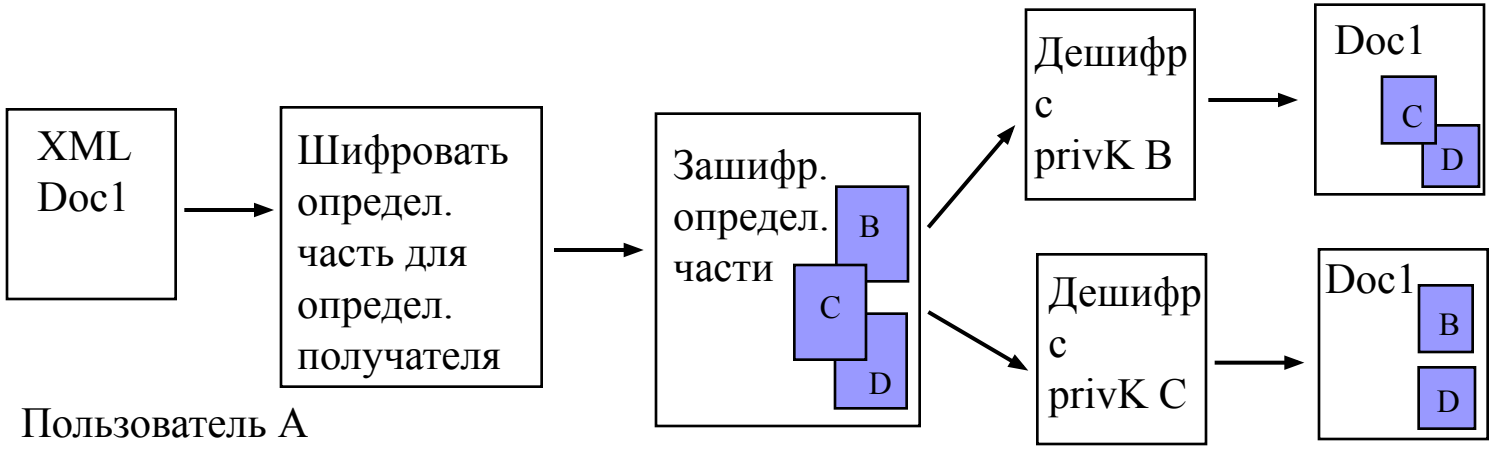
- XML-документ может иметь длинную историю, при этом различные части документа могут создаваться и «визироваться» различными субъектами и в различное время
- Различные стороны/субъекты могут иметь полномочия подписывать только различные части документа
- Позволяет сохранять целостность одних частей документа и иметь возможность изменять другие части документа
- Позволяет присоединять маркеры/мандаты безопасности к документу в отличие от использования безопасного соединения клиент/сервер
- XML-подпись обеспечивает сервисы безопасности для протоколов, основанных на XML
  - А также основу для включения информации о состоянии, контексте безопасности, истории (принятия решений)

Шифрование файла и XML-шифрование



Пользователь A
(знает pubK B)

Только пользователь B может прочитать FileA при помощи privK B



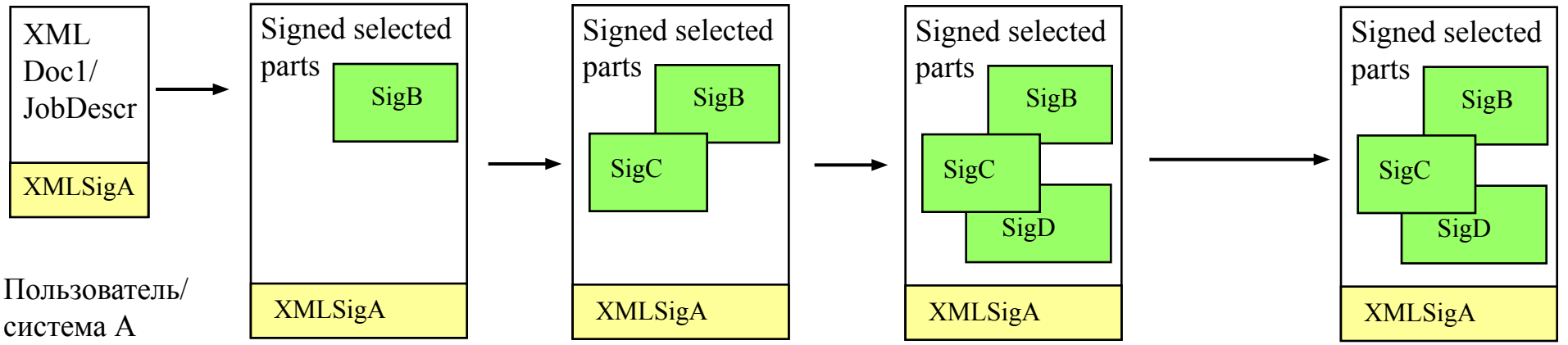
Пользователь A
(знает pubK B,C, D)

Пользователь B может проочитать весь Doc1 и дешифровать только часть B

Пользователь C может прочитать весь Doc1 и дешифровать только часть C

Для много-пользовательского шифрования Document может содержать ключ для дешифрации (симметричный или асимметричный), зашифрованный при помощи OK всех целевых получателей

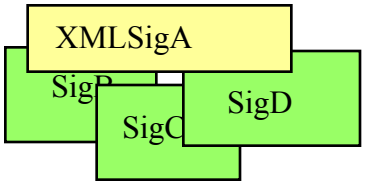
Связывание атрибутов с документом при помощи XMLSig



Пользователь/ система A создают XML Doc1 и подписывают его с SigA

Пользователи B, C, D подписывают определенные части документа своими секретными ключами privK B, C, D

- Новая информация может быть добавлена и документ подписан в целом
- Подпись может также включать другие подписи



Получатель проверяет целостность XML Doc1 посредством контроля цифровых подписей

XML Signature позволяет подписывать отдельные части документа

- Основа для аутетичности и целостности (Integrity and Authenticity)
- Связывание атрибутов безопасности и прав с документом или его частями

Современная архитектура сервисов AuthN и AuthZ

Требования к современной архитектуре AuthN/Z

- Разделение сервисов аутентификации (AuthN) и авторизации (AuthZ)
  - Аутентификация в «домашней»/«родной» организации
  - Авторизация осуществляется ресурсом
- Конфиденциальность, приватность и анонимность
- Управление доступом на основе ролей (RBAC – Role Based Access Control) и использование политики доступа

Проблемы

- Множество логинов/паролей – на каждый ресурс/сайт
- Ограничение одним доменом безопасности или множество сертификатов открытых ключей
- Сложность частичной динамической делегации полномочий

Базовые технологии

- LDAP директории и метадиректории для хранения данных о пользователях
- Собственные системы авторизации

Актуальность: AuthN/AuthZ в научных и образовательных сетях

- Доступ к многосайтовым веб/Интернет ресурсам
  - Перенаправление + cookie (SSO)
- Межуниверситетские ресурсы и доступ к внешним ресурсам или предоставление доступа для внешних пользователей
  - Например, библиотечные каталоги или научные БД
- Распределенные университетские кампусы и дистанционное обучение
- Грид-центры и Грид-приложения

- Общие характеристики/проблемы
  - Различные административные домены и домены безопасности
  - Единый доступ (SSO – Single Sign On) и множество паролей
  - Разделение идентификации/аутентификации и управления доступом

Использование LDAP в сервисах AuthN/AuthZ

Структуры персональных данных в LDAP

- Person (RFC2256), organisationalPerson (RFC2256), InetOrgPerson (RFC2798)
- EduPerson – расширение для образовательных организаций

Основные атрибуты Person objectClass

- sn/surName
- cn/commonName
- givenName
- uid, displayName
- **userPassword**
- x500uniqueIdentifier
- userCertificate
- userSMIMECertificate
- userPKCS12
- postalAddress
- o/organizationName
- ou/organizationalUnitName
- st/stateOrProvinceName
- l/localityName
- c/country
- title,employeeType
- mail
- photo

Дополнительные атрибуты EduPerson (всего 43)

- eduPersonAffiliation
- eduPersonNickname
- eduPersonOrgDN
- eduPersonOrgUnitDN
- eduPersonPrimaryAffiliation
- eduPersonPrincipalName
- eduPersonEntitlement
- eduPersonPrimaryOrgUnitDN

Управление доступом на основе ролей

RBAC – Role Based Access Control - http://csrc.nist.gov/rbac/

- Роль описывает функцию и определяет права/привилегии
- Права определяют доступ к ресурсу в определенном режиме

Преимущества RBAC

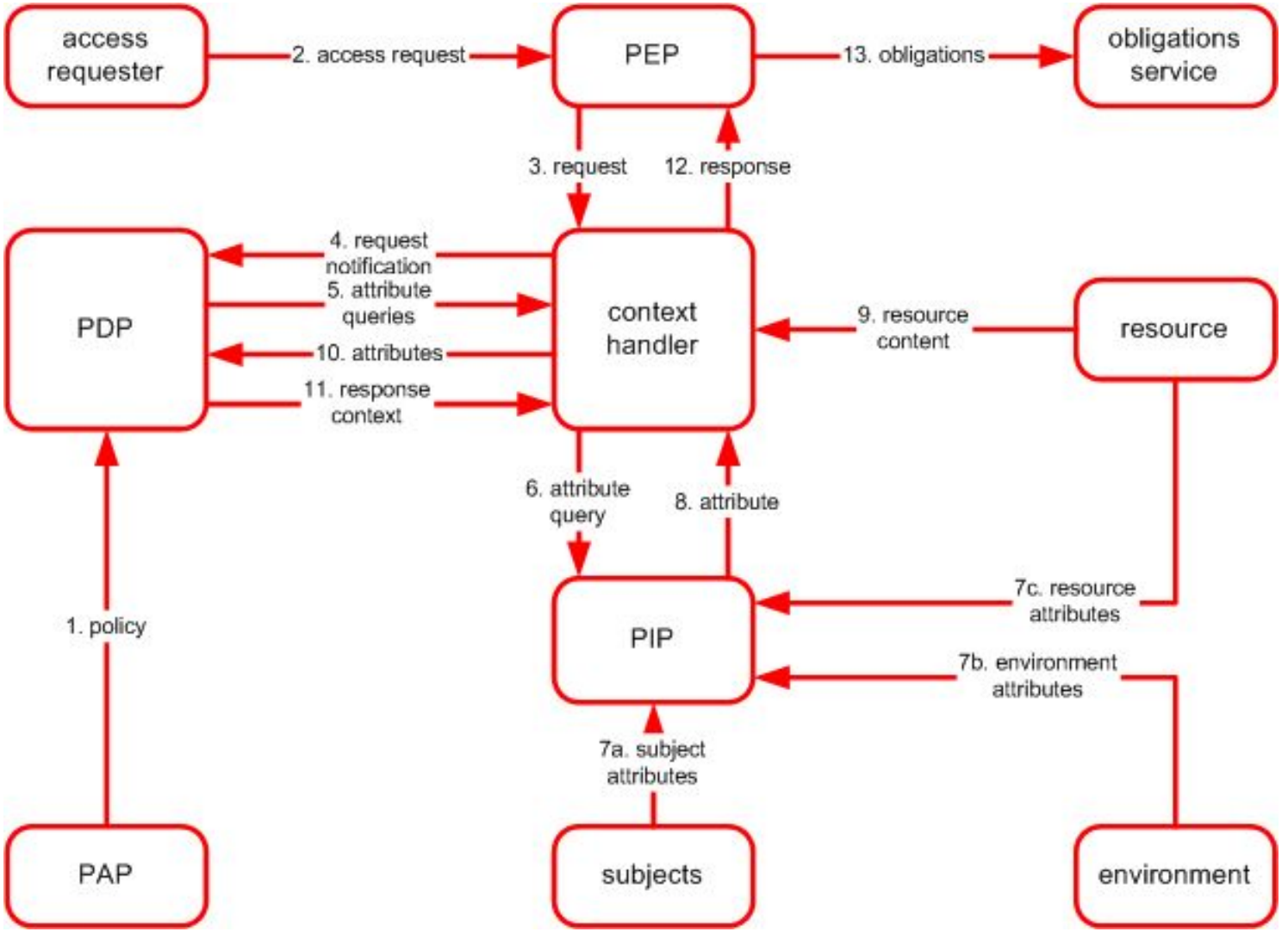
- Легко управлять и контролировать
- Раздельное назначение роли-пользователи и роли-привилегии
- Масштабируемость и иерархия
- Поддерживает принцип минимально необходимых привилегий
- Наследование и агрегирование привилегий/прав
  - Новая роль может включать комбинацию уже существующих ролей с их правами
- Упрощает процедуру делегирования

Инфраструктура управления привилегиями

PMI – Privilege Management Infrastructure (ISO/IEC 10181-3)

- Строится на основе Сертификатов Атрибутов (AC – Attribute Certificate)
- AC совместно с СОК определены стандартом X.509 version 4
  - СОК используется для аутентификации, AC используется для авторизации
- PMI как основа для построения RBAC
  - AC позволяет связать идентификатор пользователя с ролями и роли с привилегиями
  - Поддерживает иерархические системы RBAC, предоставляя возможность обьединения роли и дополнительных привилегий
  - Ограничивает глубину делегирования
- Политика PMI
  - Используется для контроля доступа к ресурсам на основе ролей
  - Правила определения ролей для пользователей и привилегий для ролей
  - Раздельные политики для субьекта, иерархия ролей, делегирование, др.

Основные компонены и потоки информации в PMI



PEP (Policy Enforcement Point)/
AEF (authorisation enforcement function)

PDP (Policy Decision Point)/ADF (authorisation decision function)

PIP (Policy Information Point)/AA (Attribute Authority)

PA – Policy Authority

Свободно распространяемые средства для AuthN/AuthZ

Разработаны в рамках проектов Internet2, FP5 и национальных научных сетей

- A-Select - http://a-select.surfnet.nl/
- Shibboleth - http://shibboleth.internet2.edu/
- PAPI - http://www.rediris.es/app/papi/index.en.html
- PERMIS (PrivilEge and Role Management Infrastructure Standards validation) - http://www.permis.org/
- SPOCP - http://www.spocp.org/

Для GRID-приложений

- VOMS – Virtual Organisation Management System
- GAAA Toolkit – http://www.aaaarch.org/

A-Select - http://a-select.surfnet.nl/

A-Select представляет собой распределенную систему веб-доступа (weblogin) с использованием cookie

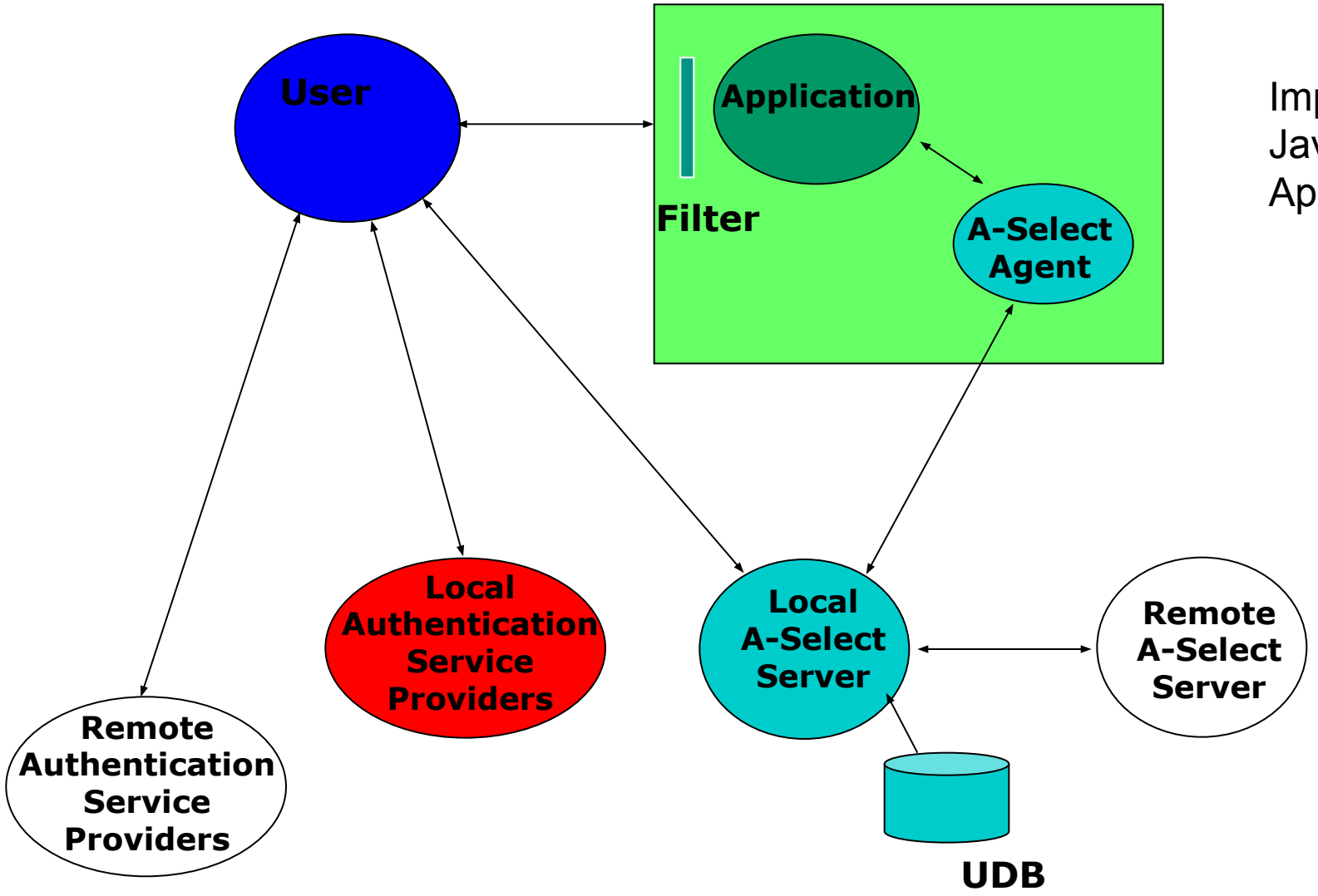
- Поддерживаемые методы аутентификации
  - IP address
  - User/password через RADIUS
  - Банковская карточка (с режимом Internet banking – SMS/TAN, Challenge generator)
  - SMS (mobile phone)
  - LDAP
  - PKI (в перспективе)

A-Select использует квитанции, которые содержат пользовательские мандаты/удостоверениюю. Два типа квитанций:

  - Квитанция, гарантирующая квитанцию ("ticket granting ticket"), выдаваемая после успешной аутентифиации ASP, and
  - Квитанция придложения ("application ticket"), которая выдается приложением, использующим A-Select.
- Единый доступ (Single-Sign-on) обеспечивается за счет назначения более длительного периода жизни для квитанция, гарантирующая квитанцию
- Квитанции A-Select реализованы как не-постоянные (non-persistent) cookie, которые сохраняются в браузере пользователя и видимы только для целевого сервиса или сервера

Разработка SURFnet - http://www.surfnet.nl/

Компоненты A-Select



Impl. Platform:
Java
Apache Tomcat 4.5/5

Вопросы и комментарии?