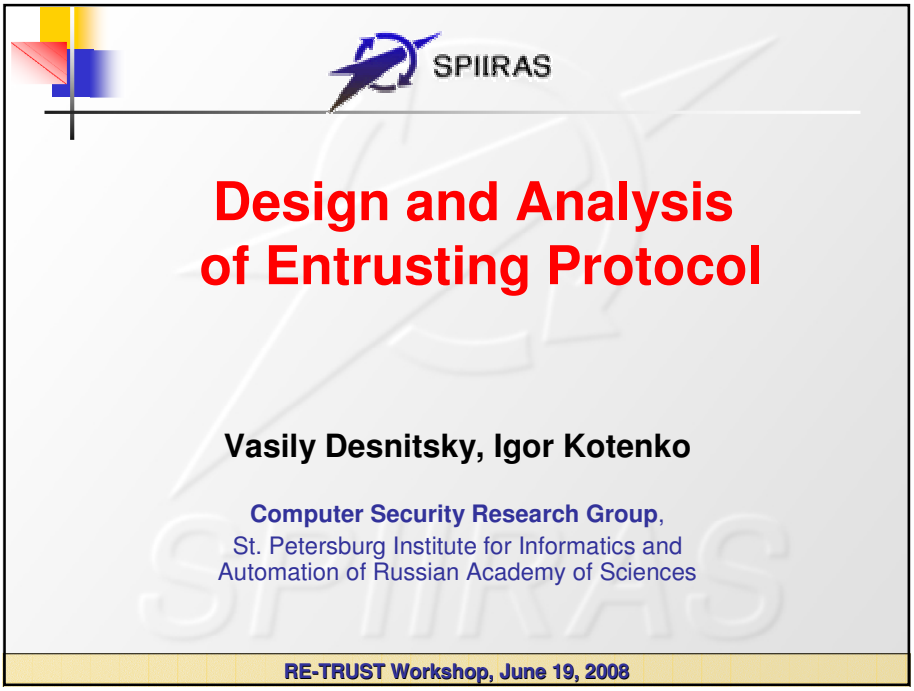
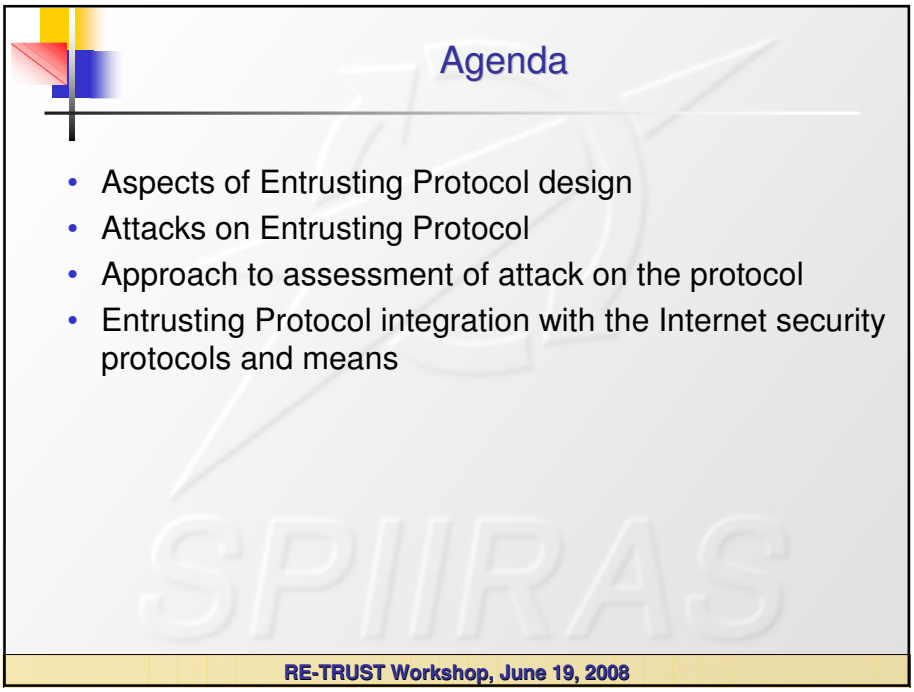
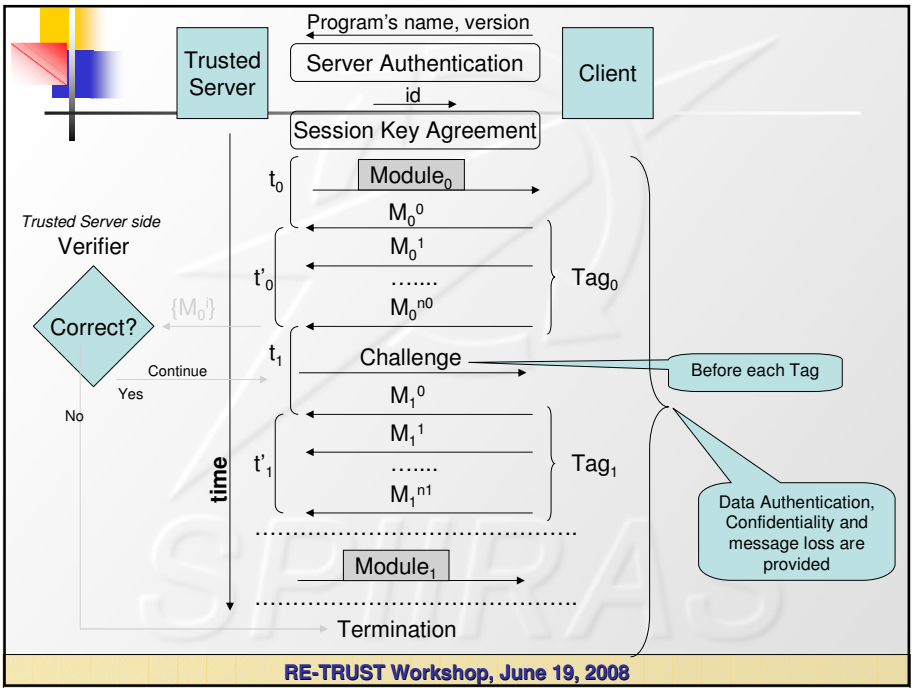

SPIIRAS
Design and Analysis
of Entrusting Protocol
Vasily Desnitsky, Igor Kotenko
Computer Security Research Group,
St. Petersburg Institute for Informatics and
Automation of Russian Academy of Sciences
RE-TRUST Workshop, June 19, 2008


Agenda
• Aspects of Entrusting Protocol design
• Attacks on Entrusting Protocol
• Approach to assessment of attack on the protocol
• Entrusting Protocol integration with the Internet security protocols and means
RE-TRUST Workshop, June 19, 2008

Entrusting protocol modeling

- Model of abstract channels
  - order
- Authentication of parties
- Key Agreement
- Confidentiality
- Data Authentication
- Message Loss
- Timeliness



Intruder Model

- Classification of attack on entrusting protocol by the type of effect
  - man-in-the-middle attacks
  - man-in-the-end attacks

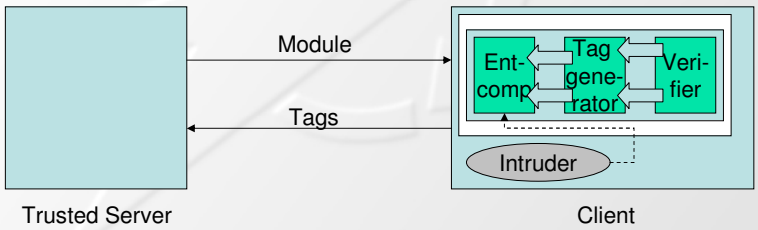
Entrusting protocol attacks (1/2)

- Attack classification by the type of intruder aims
  - Eavesdropping of the communicational channels
  - Traffic modification
    - Outgoing client traffic modification (i.e. modification of tags)
    - Ingoing client traffic modification (i.e. modification of modules)
  - DOS attacks
    - Integrity violation
    - Traffic prohibition

Entrusting protocol attacks (2/2)

- Attack properties
  - Level of attack stealthiness (attack discovery complexity)
  - Time complexity of attacks
  - Automation possibilities

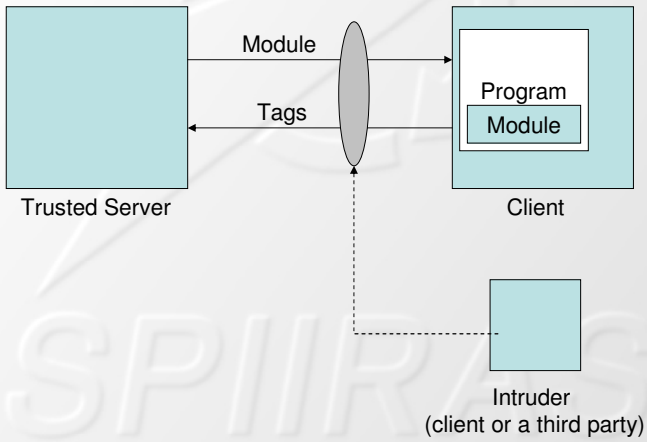
Man-in-the-end model



Man-in-the-end attacks to the protocol

- Two different attack types
  - Malicious influence on the entrusting protocol component on the client side
    - Eavesdropping some specific data (e.g. secret keys, which aren't transmitted in the net) (and its modification if reasonable)
    - Modification of the protocol rules, when having some lower-layer protocol vulnerabilities (for the trusted server not to reveal such modification)
  - Eavesdropping of client's host gateway (equivalent to middle attack)

Man-in-the-middle model



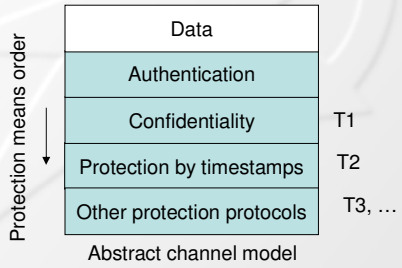
Approach to assessment of time complexity of attacks on entrusting protocol

- Consider an attack and determine all actions composing it
  - Estimation of time complexity of all *cryptographic algorithms* involved in the protocol which need to be realized by the attacker (e.g. hash function collision find, crypto analysis, etc.)
    - Getting formal evaluations from the corresponding works on crypto formal evaluation of algorithms in use
  - Estimations of some specific human-based actions of the attack (e.g. effect on the program to spy secret keys or hash functions)
    - Empirical study
- Abstract channels model use

Attack assessment example (1/2)

- The attack – eavesdropping of entrusting tags
- For the attack fulfillment the attacker needs to cope with tag *confidentiality* and the other protocols and means located in *outside* abstract channels
  - T1 = time complexity estimation of corresponding key receiving and entrusting tag decryption
  - T2, T3, … - assessments for the other, outside protection protocols

Attack assessment example (2/2)



Total time complexity T = T1 + T2 + T3 + …

Entrusting protocol Integration

- Integration the entrusting protocol with other Internet security protocols and means to reinforce it
  - Public Key Infrastructure
  - Time-stamp protocol

Public Key Certification Infrastructure (PKI) (1/2)

- PKI supports the secured exchange of data with
  - Confidentiality (symmetric bulk data encryption / hybrid encryption scheme)
  - Integrity (MAC / hash)
  - *Entity authentication*
  - Non-Repudiation
- PKI uses Public Key Cryptography to support keys and certificates
  - Generation, distribution, management and revocation of certificates associated with specific public keys
- Trust hierarchy - Hierarchical Trust Model
- PKI is relied on Trust, rather than provides it

PKI components

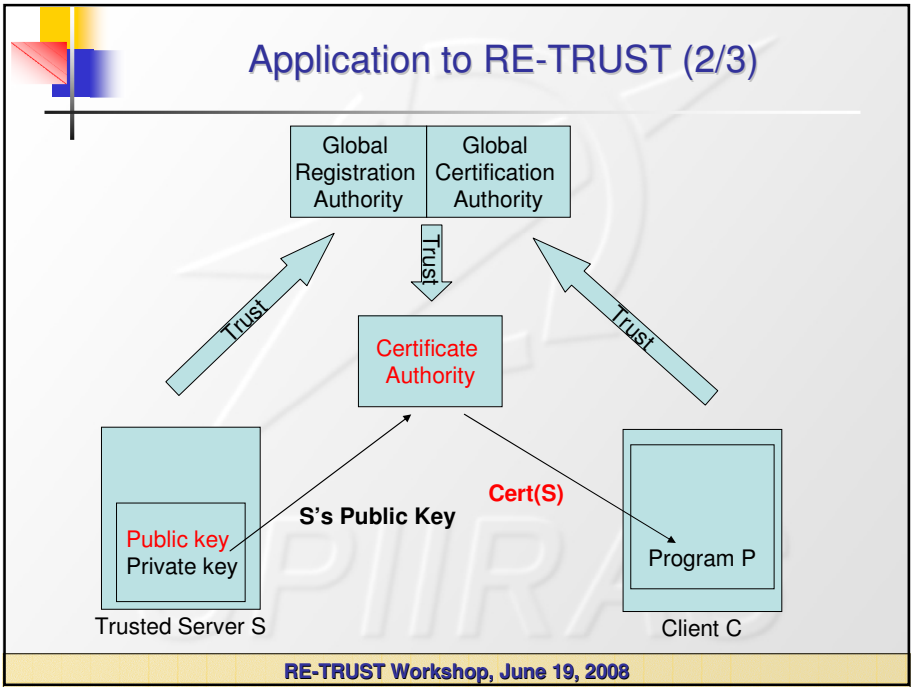
- End entities, relying entities
- Certificate authorities (CA)
- Public key certificates
- Registration authorities (RA)
- Certificate depositories
- Certificate policies
- Hardware security modules
- CA and RA could combined and could be realized as both software and hardware components

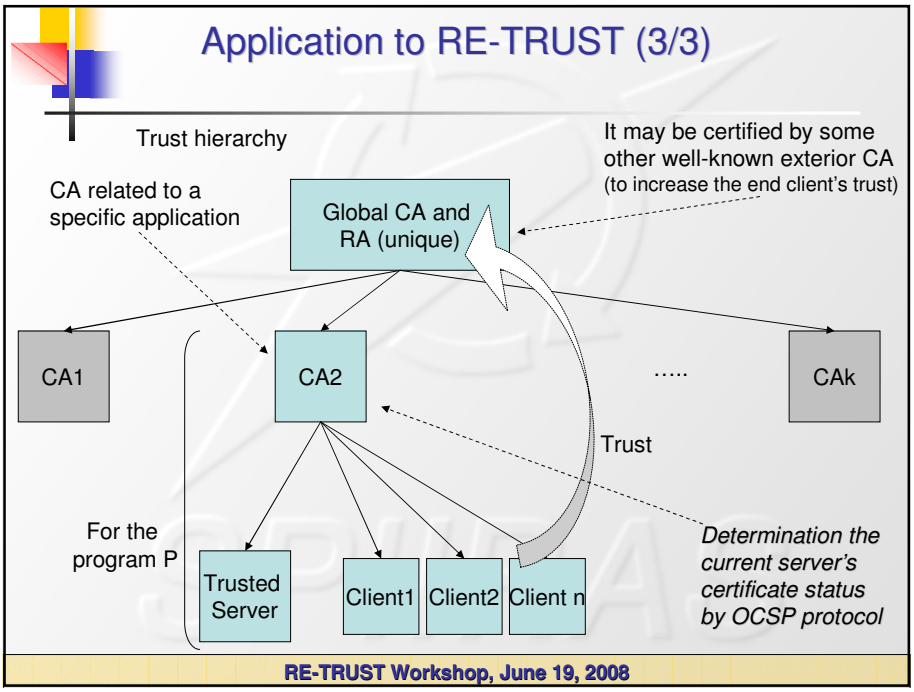
Certificates

- A digital document that binds a public key to an identity
- Public key certificate binding and signing
- Certificate validation
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
- Entity authentication

Application to RE-TRUST (1/3)

- PKI as Trusted Server Authentication Mechanism
- PKI as Client Authentication Mechanism (if required, depends on RE-TRUST authentication requirements)
- Other security services provided by PKI
  - Confidentiality
  - Message authentication (integrity)
  - Non-repudiation
  - The ability to receive any keys which may be used for the other RE-TRUST components functioning


Application to RE-TRUST (2/3)
Global Registration Authority
Global Certification Authority
Trust
Trust
Trust
Certificate Authority
Public key
Private key
S's Public Key
Cert(S)
Program P
Trusted Server S
Client C
RE-TRUST Workshop, June 19, 2008


Application to RE-TRUST (3/3)
Trust hierarchy
It may be certified by some other well-known exterior CA (to increase the end client's trust)
CA related to a specific application
Global CA and RA (unique)
CA1
CA2
.....
CAk
Trust
For the program P
Trusted Server
Client1
Client2
Client n
Determination the current server's certificate status by OCSP protocol
RE-TRUST Workshop, June 19, 2008

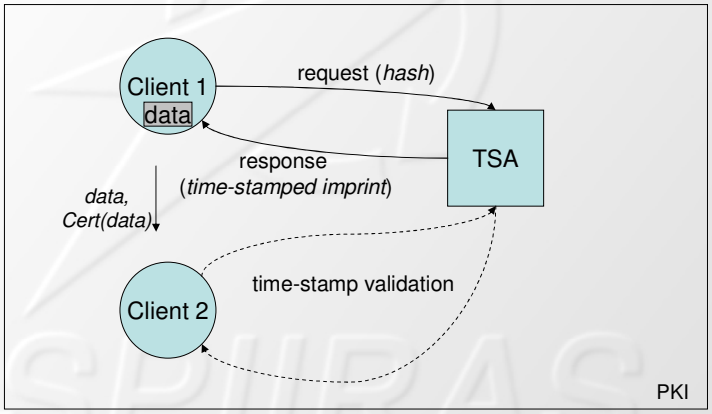
Time-Stamp Protocol (TSP)

- Cryptographic protocol for certifying timestamp providing
- Based on public key infrastructure (PKI) and X.509 certificates
- Timestamp is an assertion that some data existed at or before a particular time point
  - (*proof of existence*)
- RFC 3161 Standard

TSP components

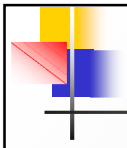
- Time Stamping Authority (TSA)
- Trustworthy source of time
- TimeStampRequest
  - Client sends data imprint (its hash value)
- TimeStampResponse
  - Client gets time-stamp certificate (data imprint and time-point) signed by TSA
- Time-stamp validation
- Time Stamping Policies

TSP scheme



TSP application

- Possible TSP application to entrusting protocol for the RE-TRUST mechanism components support
- Time Stamping use
  - When forming entrusting tags
  - To store information on the program's state on specific time points
- It makes sense to use time-stamp service for a data of long storage only (?)
  - => not applicable for entrusting tags to be time-stamped



Future work

- Further analysis of attacks on the Entrusting Protocol
- Research on other security protocols integration with the remote entrusting method
- Work on the protocol part of the program prototype
- Preparation of the material for Entrusting Protocol related deliverables (D2.5 and D4.7)