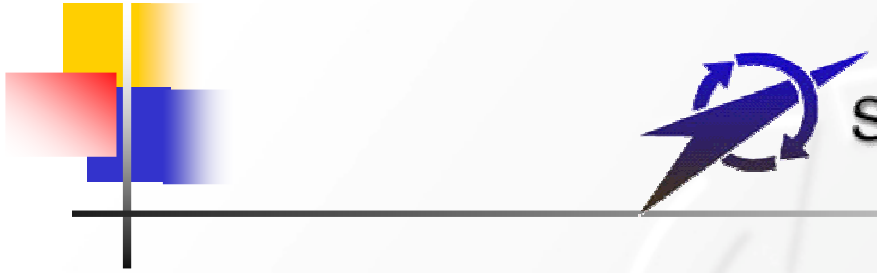


Entrusting Protocol Design: problem settlement, requirements and related protocols

Vasily Desnitsky

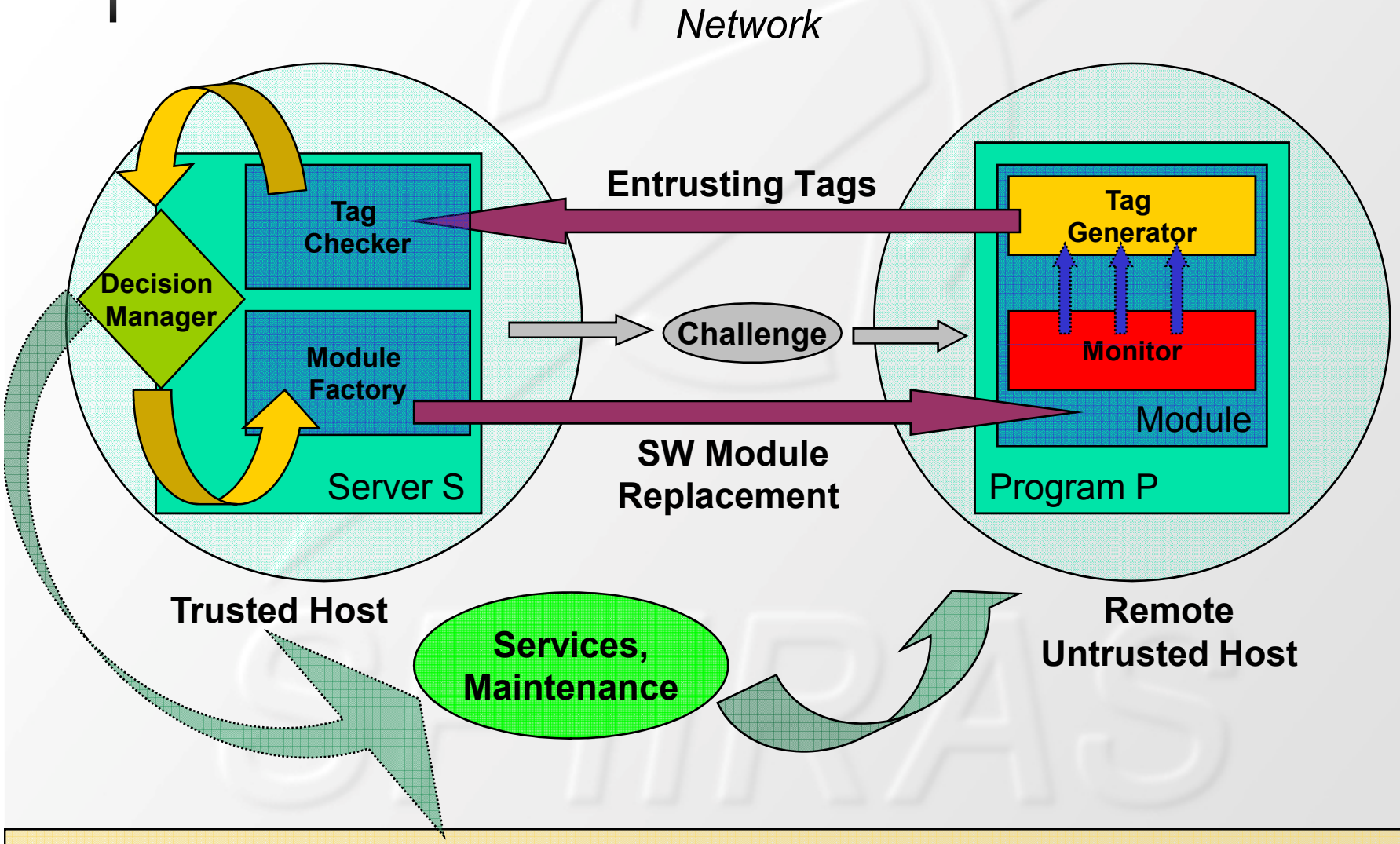
Computer Security Research Group,
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences

Protocols Investigation

- Problem settlement
- Determination of possible Attacks and related protocol requirement
- Analysis of requirements to Entrusting Protocol
- Proposals to Entrusting Protocol
- Entrusting Protocol Resistance analysis
- Getting of estimations of attack time complexity for dynamic replacement mechanism support

Current work

Reference Architecture



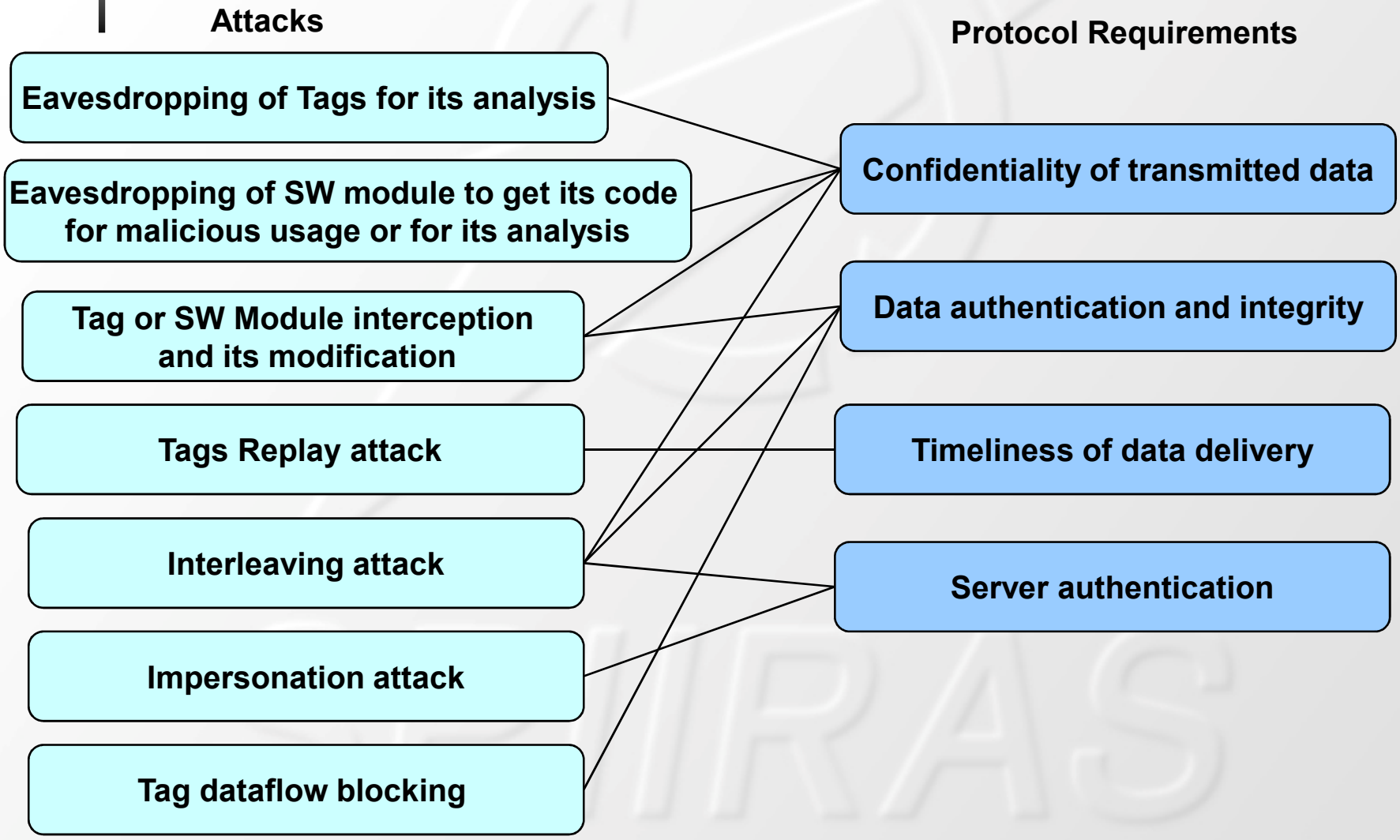
Transmitted Data

- Entrusting Tags
  - Small data portion
  - Continuous dataflow and even in time
- SW Module code
  - Occasional data sending
- Challenge from Trusted Server to Client
  - Occasional data sending
- Additional services, update, maintenance
  - Use their own protection mechanisms

Attacks

- Eavesdropping of Tags for its analysis
- Eavesdropping of SW module to get its code for malicious usage or for its analysis
- Tag or SW Module interception and its modification
- Tags Replay attack
- Interleaving attack
- Impersonation attack
- Tag dataflow blocking

Attacks and Entrusting Protocol requirements



Identification of clients

- Trusted Server needs to distinguish different clients
- To identify each running copy of the program being protected on the client
- Identification by IP address
  - Constraint: it's applicable for local area network only where IP can unambiguously determine each client
- Artificial unique identifier supplied by Trusted Server
  - Getting a new identifier after every new program start
  - No need to protect identifier

Approach to Server Authentication

- Client should have guarantee he is communicating with real Trusted Server
- The way is to find
  - some property inherent Trusted Server
  - some secret data, the secrecy meaning certain *hard computational problem*
- To construct a *knowledge proof protocol* demonstrating ownership of the secret to client

- Open question: how to discover such secret?

Confidentiality

- Guarantee of impossibility of data decoding by a malicious user
- Symmetric key schemes
  - (+) High time rate
    - Possible for implementation of Entrusting Tags, SW Module and Challenge encryption/decryption
  - (-) Necessity of secure secret key management
  - *E.g. 3DES, IDEA, AES in CBC mode*
- Public key cryptography schemes
  - (-) Low time rate
    - Possible for Entrusting Tags and Challenge
  - (-) Necessity of guarantee of public key authenticity by a specific certificating entity
  - E.g. *RSA*
- Hybrid cryptosystems
  - Combination of symmetric and public key encryption
    - Possible for Entrusting Tags, SW Module and Challenge

Data Authentication and Integrity

- To be able to determine if this subject is the author of given data
- To prevent a malicious user to forge or modify transmitted data
- Data authentication assumes data integrity
- Message Authentication Codes (MAC) for symmetric schemes
  - Use hash-function based on shared secret key
- Digital signature for public key schemes
- Encrypt-then-authenticate
- Authenticated encryption
- Digital signature schemes giving message recovery

Timeliness

- Requires to deliver Entrusting Tags and SW Module in specific time
- To verify the tag was generated and sent no later than certain time instant
- 1 strategy: validity window determination
  - Forced delays in Tag Generation and Delivery Process
    - Network characteristics (determination be specific request to client)
    - SW Module characteristics (e.g. verification function amount)
    - Program being protected characteristics (e.g. program's size, memory volume in use, etc.)
    - characteristics of client's HW resources and OS
- 2 strategy: to tie information to its creation time instant
  - Algorithm of tag creation should depend on time
  - Capability to check creation time of Tags

Message loss

- In case of one message loss Trusted Server immediately start to consider client program as tampered

- Possible means
  - Superfluity – information doubling
  - Server reaction – request to Client to repeat the message
  - Low layer protocol support

Protocol Design Issues

- Need of protection on Network layer
- Suggestion
  - To implement Entrusting Protocol as Application layer protocol over secure network layer protocol
- Two proposals:
  - Internet Security Protocol (IPSec)
  - Secure Sockets Layer (SSL)

IPSec Protocol

- Network layer protocol providing
  - Data Authentication and integrity
  - Secrecy (confidentiality) – encryption of IP-packets
  - Replay attack prevention

- Authentication Header protocol (AH)
- Encapsulating Security Payload protocol (ESP)
- Internet Key Exchange Protocol (IKE)
- IP Payload Compression Protocol (IPComp)
- Transport and Tunnel modes

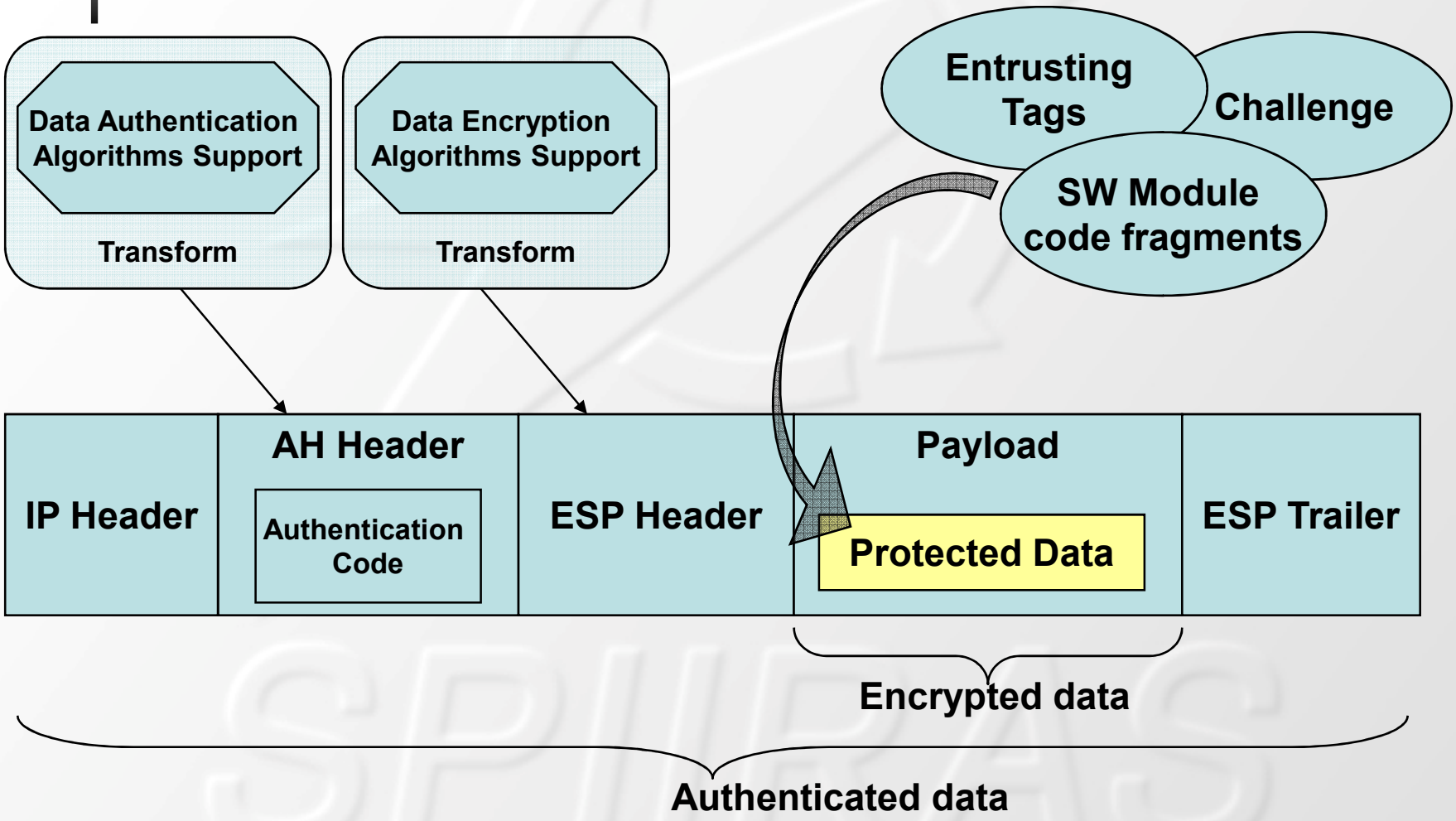
Data Authentication and Confidentiality in IPSec

- Authentication Header
  - Security Parameter Index (SPI)
  - Authentication Code
  - Sequence Number
- Encapsulating Security Payload
  - SPI
  - Sequence Number
  - Payload
  - Authentication Code
- Internet Key Exchange Protocol (IKE)
  - To agree cryptographic algorithms and shared secret keys
  - Modification of keys during protocol act

Application of IPSec to Entrusting Protocol (1/2)

- Combination of AH and ESP for IP-packet protection
  - AH – integrity and authentication of IP packet including IP header
  - ESP – IP packet payload confidentiality
- Transport mode use
- AH doesn't protect mutable fields from IP header
- IPSec doesn't depend on concrete cryptographic algorithms in use. It allows to add new cryptographic algorithms when they appear

Application of IPSec to Entrusting Protocol (2/2)



Approach to Resistance Analysis of IPSec based proposal

- AH and ESP headers contain Transforms, that hide all cryptographic concerns
- Resistance of AH and ESP against attacks in the first place means resistance of cryptographic algorithms in use

- IKE protocol is very tangled and hard to analyze
  - In contrast to AH and ESP all cryptographic concerns are implemented within IKE

Secure Sockets Layer Protocol (SSL)

- SSL provide
  - Integrity
  - Data authentication
  - Confidentiality
- SSL is implemented within Transport Layer protocol
- Two levels of SSL:
  - SSL Handshake Protocol – allows to agree cryptographic algorithms and keys
  - SSL Record Protocol – provide secure encapsulation of implemented high layer protocol (e.g. HTTP, LDAP, IMAP)

Application of SSL to Entrusting Protocol

- SSL is compatible with all contemporary proxy servers and routers
- Use of cipher block chaining (CBC) for data encryption
- Possibility of change of encryption specification during protocol fulfillment (protocol of cipher specification modification)

Future work

- Analysis of Entrusting Protocol Resistance
- Analysis of attacks on Entrusting Protocol
- Getting of estimations of attack time complexity for dynamic replacement mechanism support