Security Issues in OPES - Threats and Risks

draft-ietf-opes-threats-00.txt

55th IETF

Atlanta, GA

B. Srinivas

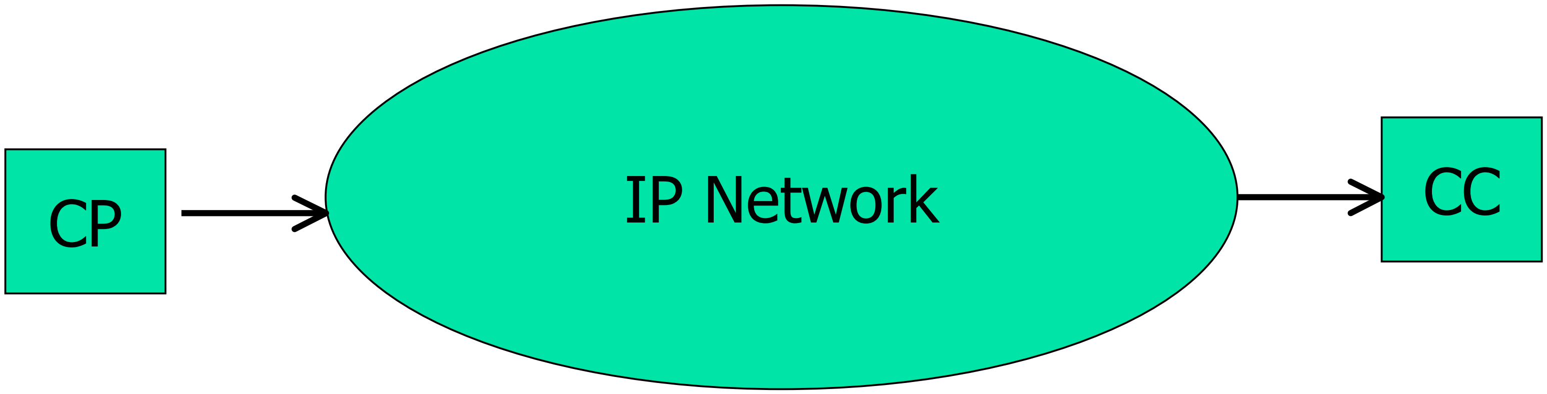
NRC Boston, Burlington, MA

Outline

- Security issues in OPES
- Based on preliminary individual ID (draft-srinivas-opes-threats-00.txt)
- In-band threats
- Out-of-band threats

Traditional vs OPES (I)

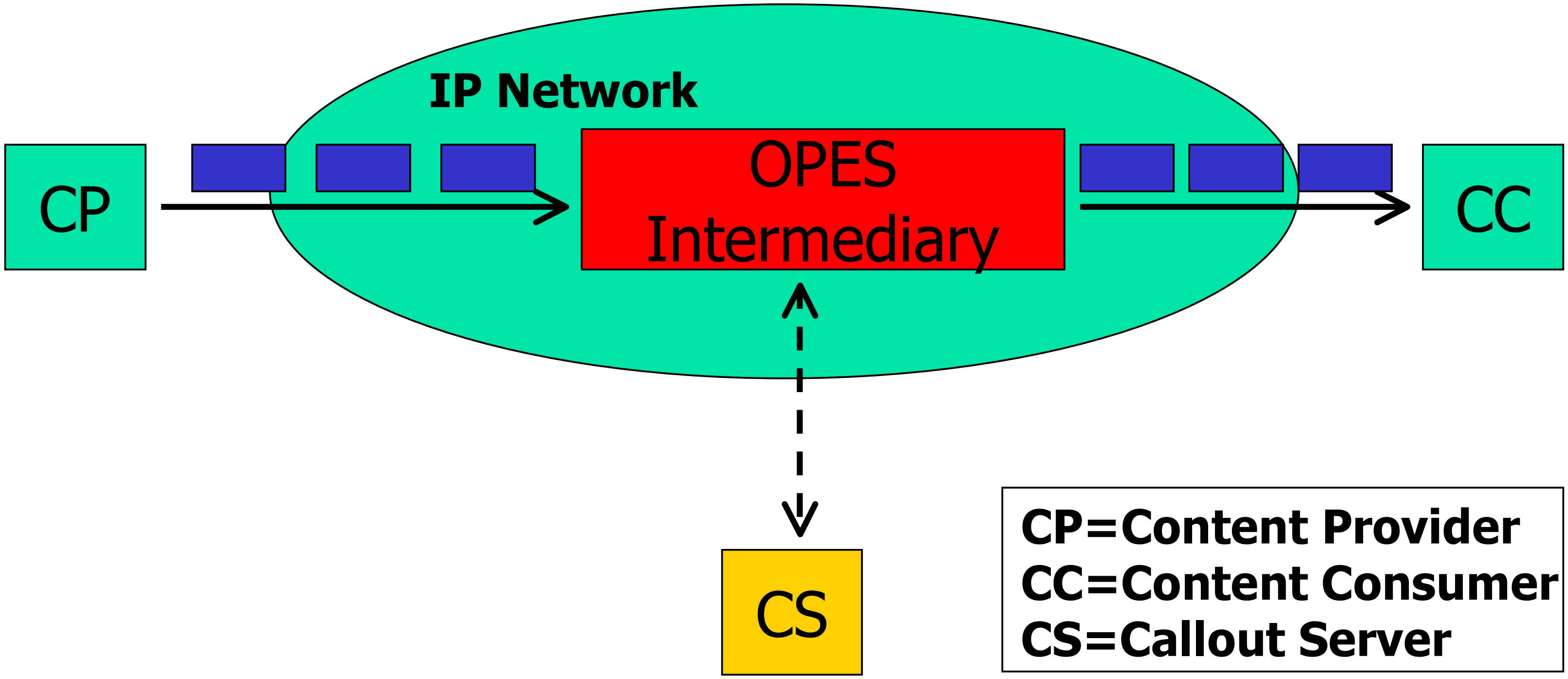
Traditional Network



CP=Content Provider
CC=Content Consumer

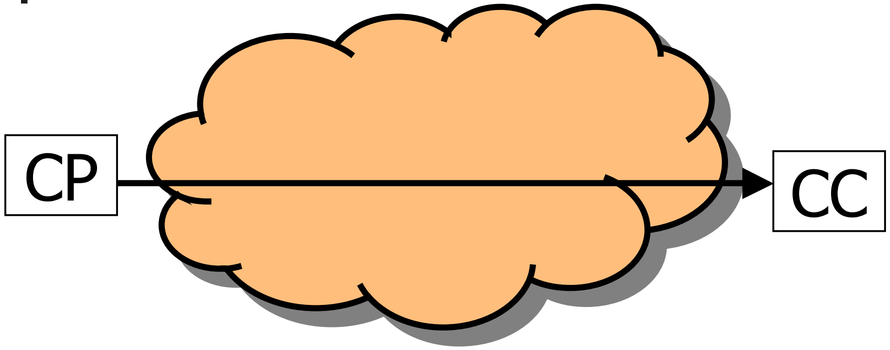
Traditional vs OPES (II)

OPES Network

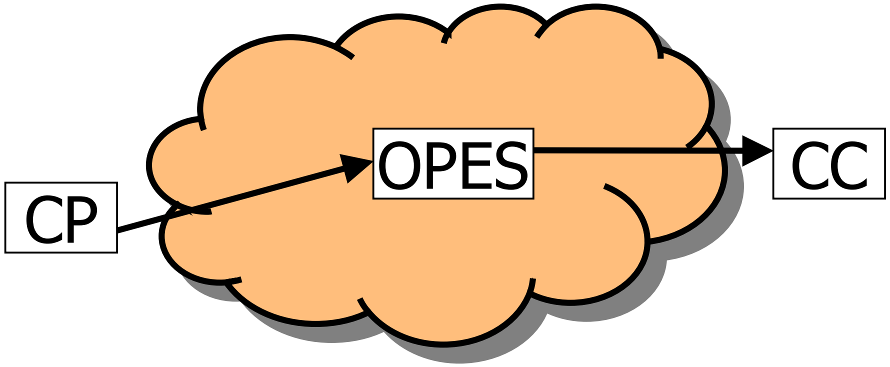


CP=Content Provider
CC=Content Consumer
CS=Callout Server

Security threats/risks in OPES



End-to-end Encryption



Hop-by-hop Encryption

- Data stream:
  - Content stream and
  - Signaling stream
- OPES introduces new site for exposure to threats by attacker
- Only hop-by-hop security, inherently less secure than end-to-end techniques, can be used in OPES

OPES Security Threats Draft

- Discusses threats on data and control and their effects
- Threats discussed congruent with security considerations raised in RFC3238
- Security risks affect both CC and CP applications.
- Threats impact quality and integrity of data produced or consumed
- Threats introduced by existence of OPES processor and callout servers

OPES Security Threats

- Types of OPES Security Threats:
  - OPES in-band data flow threats
    - OPES Flow Network Level Threats
    - OPES Flow Application Level Threats
  - Out-of-band data or control information flow threats

OPES In-band Data Flow Threats

- Broadly classified into two types:
  - OPES Flow Network Level Threats
  - OPES Flow Application Level Threats
- Threats to trust in OPES network:
  - Insider – caused by parties part of OPES system
  - Outsider – caused by parties not part of OPES system
- Trust based on transitive trust between CP, OPES entities and CC

OPES Flow Network Level Threats – A Listing

- OPES/callout device spoofing
- Remote callout device spoofing
- Session hijacking
- Data Confidentiality
- Denial-of-Service (DoS)
- Threat to network robustness

OPES/Callout Device Spoofing

- THREAT:
  - Malicious node masquerades as OPES device, or
  - Genuine OPES device, but malicious callout server

- EFFECT:
  - Malicious node:
    - eavesdrops on traffic between CP and CC
    - forces either end-point to use expensive or undesired services
    - doesn't forward traffic, resulting in a DoS attack

Remote callout server spoofing

- REMOTE = Callout server and OPES device in different administrative domains
- THREAT:
  - Despite OPES device authentication, malicious data transformation performed in remote callout server
- EFFECT:
  - Similar to those produced by malicious OPES device/collocated callout server (see previous slide)

Session Hijacking

- THREAT:
  - A TCP/IP session is hijacked by an attacker

- EFFECT:
  - Integrity of content on an OPES device is compromised by the hijacker

Data Confidentiality

- THREAT:
  - Snoop on fields within messages
  - Eavesdrop on content messages
  - Can garner topology/location/IP address information
  - Snoop on usage information including logging, monitoring for debugging and billing purposes
  - Eavesdrop on security related information exchanged between CP and CC

- EFFECT:
  - Information not to be divulged is divulged
  - Eavesdropping on security related information compromises integrity of subsequent content data exchange

Denial-of-Service (DoS)

- THREAT:
  - Legal data traffic denied needed traffic resources due to overloading of OPES device by spurious service requests
  - Resources: CPU cycles, memory, network interfaces …
  - Distributed DoS caused by attacker directing multiple nodes to launch DoS attacks simultaneously
  - DoS attack can be:

    1) Selective 2) Generic 3) Random
- EFFECT:
  - Legal data traffic unable to obtain OPES services
  - Acting as a DoS component, malicious OPES intermediary interrupts data flow between CP and CC

Threat to Network Robustness

- THREAT:
  - Violates end-to-end addressing principles
  - Not use flow-control for managing connections
  - Interferes with flow control of connections it did not originate
- EFFECT:
  - Endanger internet infrastructure by complicating routing and connection management
  - Defeats many protective mechanisms and safeguards built into OPES architecture
  - Could cause Internet congestion

OPES Flow Application Level Threats

- Unauthorized OPES entities
- Unauthorized actions of legitimate OPES entities
- Unwanted content transformations
- Corrupted content
- Message structure integrity
- Granularity of protection
- Hop-by-hop vs end-to-end protection
- Integrity of complex data
- Denial of Service (DoS)
- Tracing and notification information

Unauthorized OPES Entities

- OPES mandates one party authorization
- OPES device authorization occurs out-of-band
- THREAT:
  - Discovering presence of an OPES entity and verifying authorization may present a problem
- EFFECT:
  - Unauthorized OPES entity may be a malicious entity
  - Malicious entity can wreak havoc on data flow between CP and CC

Unauthorized Actions of Legitimate OPES Entities

- Requesting permission from CP/CC for each rule and procedure is cumbersome
- Instead, authorization given for class of transformations
- THREAT:
  - Actual triggered procedures may maliciously perform unauthorized actions
- EFFECT:
  - Such actions can result in improper and undesired content transformation

Unwanted Content Transformations

- THREAT:
  - Authorized OPES service may perform actions that do not adhere to the expectations of the party that gave the authorization
  - Alternatively, OPES entity acting on behalf of one party may perform transformations that another party deems inappropriate
- EFFECT:
  - Undesired content transformation may negate the utility of the data flow between CP and CC

Corrupted Content

- THREAT:
  - Malicious attack causes OPES system to deliver outdated or otherwise distorted information
- EFFECT:
  - May introduce changes causing improper actions in OPES server or callout server
  - These changes may be in message body, headers or both

Message Structure Integrity

- THREAT:
  - OPES server may add, remove or delete certain headers in a request and/or response message
- EFFECT:
  - Such changes may violate end-to-end integrity requirements
  - Also, such changes defeat services that use information provided in such headers

Granularity of Protection

- Content modification permission applies to portions of content
- Policies needed to refer to portions of messages and to detect modifications
- THREAT:
  - Little support for policies expressed in message parts
- EFFECT:
  - Cannot detect problems inherent in hop-by-hop data integrity measures
  - Difficult to attribute particular modification to particular OPES processor
  - Inability to automatically detect policy violations

Hop-by-hop vs end-to-end protection

- OPES data must be transmitted:
  - Without confidentiality protection, or else
  - With hop-by-hop encryption
- THREAT:
  - A malicious processor in the path can manipulate keys on that hop
  - Use of weak cryptography or poor key management in delivery path
- EFFECT:
  - By manipulating keys in some hop, confidentiality and integrity of data can be compromised without detection
  - Modifications by unauthorized parties
  - Danger of data leakage

Integrity of Complex Data

- THREAT:
  - OPES system may apply inconsistent transformations to interrelated data objects or references within the data object
  - Deliberate replacement/deletion/insertion of links
- EFFECT:
  - Such inconsistent transformations violate data integrity
  - Replacement/deletion/insertion of links may violate intentions of the CP

Tracing and Notification information

- THREAT:
  - Inadequate or vulnerable implementation of the tracing and notification mechanisms
  - Such facilities may become a target of malicious attack
- EFFECT:
  - Defeats safeguards built into OPES
  - Creates problems in discovering and stopping other attacks

Threats to Out-of-band data

- Threats to OPES in-band data flow
  - Caused by weakness in implementation for:
    - Security
    - Authentication
    - Authorization
  - Threats described in previous set of slides
- Threats to out-of-band data integrity

Threats to Out-of-band Data Integrity

- Inaccurate Accounting Information
- OPES service request repudiation
- Exposure of private information
- Inconsistent privacy policy
- Exposure of privacy preferences
- Exposure of security settings
- Improper enforcement of privacy and security policy

Inaccurate Accounting Information

- THREAT:
  - Distortion or destruction of base or processed accounting data challenges accounting functionality
- EFFECT:
  - CC wrongly charged for viewing content not successfully delivered
  - CP or independent OPES service provider not compensated for services performed
  - Attack on accounting system may result in incorrect resource management and DoS by artificial resource starvation

OPES service request repudiation

- THREAT:
  - CP or CC, initially authorizes an OPES intermediary to perform a service, later denies making it
- EFFECT:
  - OPES intermediary MAY be held liable for unauthorized changes to the data flow

Exposure of Private Information

- THREAT:
  - Private information of CC inadvertently or maliciously exposed
  - Includes passwords, buying patterns, page views, and credit card numbers
  - May also include logs and accounting data
- EFFECT:
  - CC subject to malicious actions by exposure of private information

Inconsistent Privacy Policy

- THREAT:
  - Privacy policy of OPES entities may not be consistent with CC or CP expectations
  - Privacy related problems further complicated when OPES entity, CP and CC belong to different jurisdictions
- EFFECT:
  - CC unaware that he/she does not have expected legal protection
  - CP may be exposed to legal risks due to failure to comply with regulation which he is not even aware of

Exposure of Privacy Preferences & Security Settings

- THREAT:
  - OPES system may inadvertently or maliciously expose end user privacy settings and requirements
  - OPES system may expose end user security settings when handling request and responses
- EFFECT:
  - Exposure of privacy preferences or security settings to a malicious entity enables possible session hijacking and other forms of attack

Improper Enforcement of Privacy and Security Policy

- THREAT:
  - Danger that these policies are not properly implemented and enforced
- EFFECT:
  - CC may not be aware that its protections are no longer in effect

Final Thoughts and Next Steps

- <draft-ietf-opes-threats-00.txt> discussed security threats and risks that a data stream is exposed to due to presence of an OPES intermediary
- Additional comments and inputs are solicited
- Teleconferences will be resumed to address raised issues