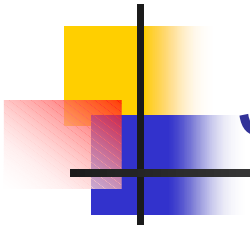
Security Threats and Risks for Open Pluggable Edge Services

`draft-srinivas-opes-threats-00.txt`

B. Srinivas Tat Chan

NRC Boston

Burlington, MA



Justifications for OPES

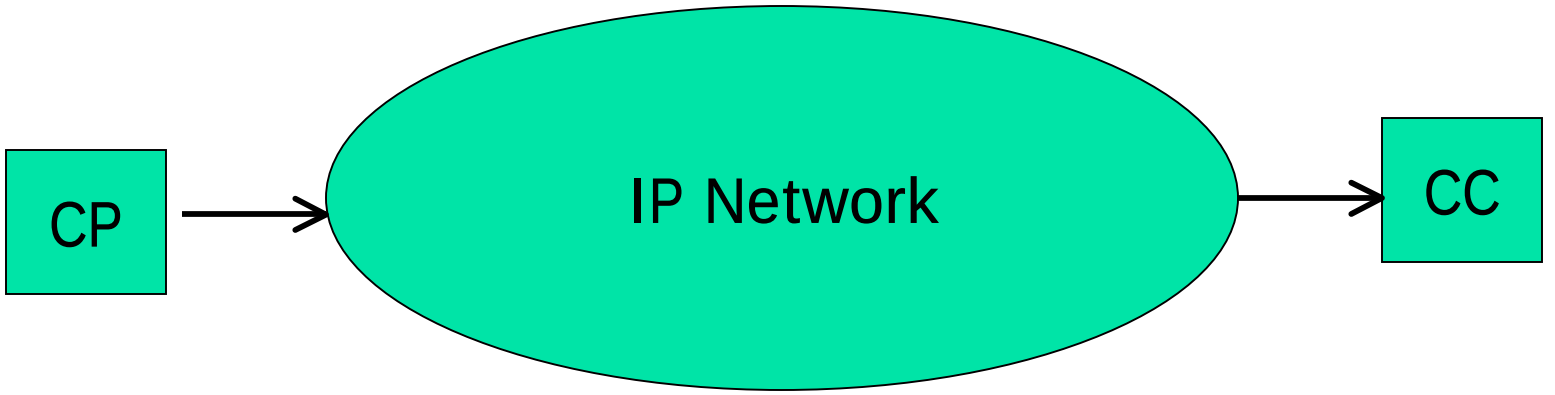
- Additional services, beyond basic networking, needed by both content providers and consumers.
- Content Services provide value-add to content.
- Examples include:
  - **Dynamic content assembly**
  - **Personalization content services (PCS)**
  - **Virus scanning**
  - **Content adaptation for different device types**

Located at the Edge

- OPES may be collocated with either end of data stream or a discrete entity situated elsewhere within network.
- Edge Service Networks (ESN) provides services listed on the previous slide.
- Service delivery rationale using ESN's:
  - Delivering at server can cause:
    - **Server overload**
    - **Increased network load**
    - **High service latency.**
  - Delivering at client possibly infeasible due to:
    - **Lack of processing power**
    - **Inability to perform software upgrades.**

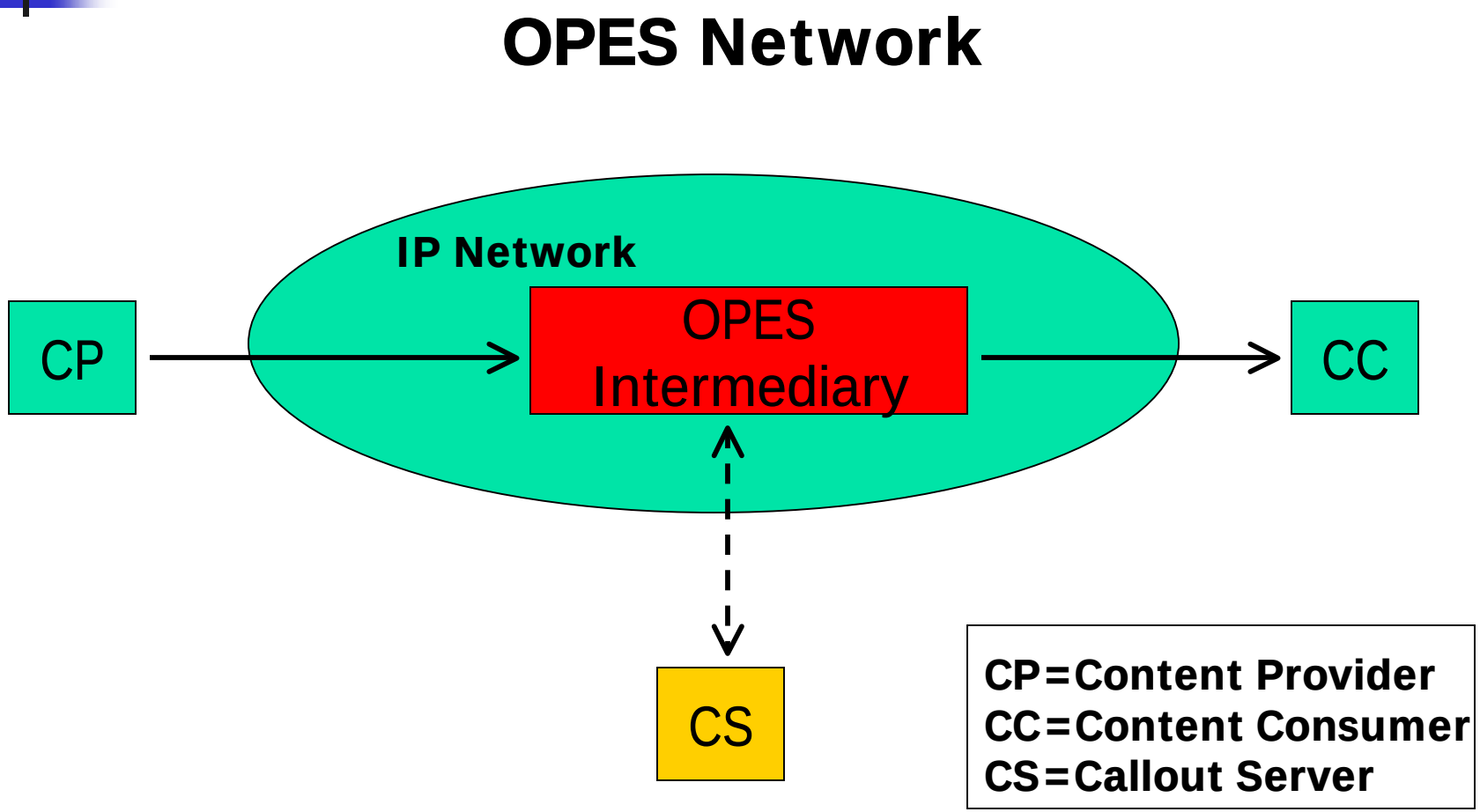
Traditional vs OPES (I)

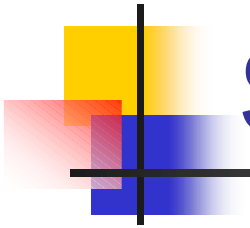
Traditional Network



CP=Content Provider
CC=Content Consumer

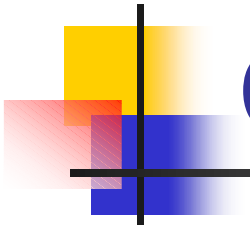
Traditional vs OPES (II)





Security Threats

- Data stream comprises both content as well as signaling streams (indicating desired transformation, for instance).
- Signaling information may originate from either CP or CC.
- Attacks on signaling and content streams may have different results and should be considered separately.
- OPES intermediary provides new functionalities thereby creating new possibilities for tampering with data traffic (content and signaling).
- Despite being authorized, OPES introduces new site for exposure to threats from malicious entities.



OPES Security Threats Draft

- Discusses array of threats, their effects and suggested security solutions.
- Threats discussed congruent with security considerations raised in RFC3238.
- Direct association between communicating end-points is broken by existence of OPES intermediaries or callout servers.
- Operation of OPES itself has security implications and risks.

A List of Threats

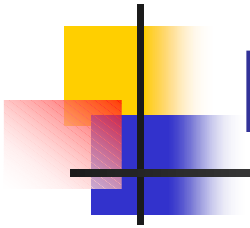
- OPES device false registration / deregistration
- OPES device spoofing
- Replay attack
- Message Integrity
- Data Confidentiality
- Denial-of-Service
- Authorized entity repudiates a request
- Re-establishing end-device - OPES device security during failover

OPES False registration / deregistration

- **THREAT:**
  - **An OPES device needs to be registered/deregistered before it can be used to provide services.**
  - **False registration / deregistration sent by malicious node on behalf of non-existent OPES intermediary.**
- **EFFECT:**
  - **End-system traffic is hijacked by malicious node.**
  - **Eavesdropping by attacker.**
  - **Unwanted or malicious transformation of data traffic.**
  - **Attacker refuses to forward data traffic to content consumer, resulting in DoS attack.**
- **SOLUTION:**
  - **A registrar MUST authenticate and authorize OPES intermediary before registering/deregistering an OPES intermediary.**

OPES device spoofing

- **THREAT:**
  - **Malicious node could send false information about intermediate device masquerading as OPES device, or.**
  - **Despite presence of genuine authenticated OPES device, actual data transformation could be performed in a malicious call-out server.**
- **EFFECT:**
  - **Similar to previous case.**
  - **Malicious node could force either end-point to use services of a malicious OPES intermediary, which renders very expensive services.**
  - **Malicious OPES intermediary may refuse to forward traffic, resulting in a DoS attack.**
- **SOLUTION:**
  - **OPES intermediary device and associated call-out server (if any) MUST be authenticated and authorized before any messages are sent through them.**
  - **End-to-end authentication through OPES device (hop by hop) using encryption and physical protection of the communication channel is required.**



Replay Attack

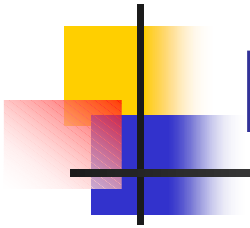
- **THREAT:**
  - **Malicious node passively eavesdrops on a communication channel and replays recorded message (signaling or data) later.**
  - **Malicious node that serves as OPES intermediary for two distinct data flows could replay message from one data flow onto another.**
- **EFFECT:**
  - **False action is performed by OPES device or call-out server.**
  - **Transformed content could be replayed as genuine content.**
- **SOLUTION:**
  - **Techniques such as sequence numbers or others, MUST be taken to prevent replay attacks.**
  - **End-to-end authentication of OPES intermediaries will protect against malicious OPES devices being used.**

End-device - OPES device security during Failover

- THREAT:
  - **When an end-device fails over from OPES intermediary A to OPES intermediary B, a trust relationship between end-device and A will not automatically translate into same relationship existing between end-device and B.**
- EFFECT:
  - **Assumption of such a trust relationship opens up security holes for malicious OPES intermediaries to perform all kinds of attacks.**
- SOLUTION:
  - **Notify application when failover occurs so that application MAY take appropriate action to establish trust relationship between end-device and B, or.**
  - **Reestablish security context transparently.**

Message Integrity

- **THREAT:**
  - **Message flow through OPES device is corrupted, implying that, message has been subject to unauthorized modification prior to OPES intermediary.**
  - **Corrupted message is inputted into OPES intermediary (or call-out server).**
  - **Signaling information or contents can be corrupted.**
- **EFFECT:**
  - **Corrupted signaling information causes OPES device to transform the content in wrong way, or.**
  - **Transforms wrong content, generating wrong output.**
  - **For OPES services, which serve to redirect content requests to different providers for load balancing, malicious node can cause redirection to overloaded or wrong provider.**
  - **Rather than concealing the identity of the requestor, a compromised OPES device may expose the same.**
- **SOLUTION:**
  - **Integrity mechanisms, such as digital signature techniques, to protect integrity of both signaling messages as well as content messages.**



Data Confidentiality (I)

- **THREAT:**
  - **Eavesdropper is capable of snooping on fields within messages in transit.**
  - **May be able to eavesdrop on the content messages being delivered to consumer.**
  - **May be able to garner different kinds of information such as topology/location/IP addresses etc.**
  - **Can eavesdrop on usage information including logging, monitoring for debugging and billing purposes.**
  - **Can eavesdrop on shared encryption keys being delivered to OPES intermediary.**

Data Confidentiality (II)

- **EFFECT:**
  - **Information not to be divulged is divulged.**
  - **Attackers can decrypt encrypted content, if shared keys are compromised.**

- **SOLUTION:**
  - **Data confidentiality service MUST be provisioned using various kinds of encryption, e.g., shared key, PKI.**
  - **Care needs to be taken in delivery of key information to OPES intermediary.**

Denial-of-Service (I)

- **THREAT:**
  - **DoS MAY be achieved by preventing data traffic from reaching intermediary or call-out server.**
  - **OPES intermediary can be overloaded by spurious service requests issued by malicious node, which denies legal data traffic the necessary resources to render service.**
  - **A malicious node, that successfully spoofs an OPES intermediary, can launch DoS attacks simply by not forwarding legitimate traffic to content consumer.**
  - **In terms of communication streams affected, DoS attack can be:**
    - **Selective**
    - **Generic**
    - **Random**
  - **Distributed DoS is possible when an attacker directs multiple nodes to initiate spurious service requests to an OPES intermediary simultaneously.**
  - **Malicious OPES intermediary can overwhelm content provider by sending numerous requests.**

Denial of Service (II)

- **EFFECT:**
  - **Legal data traffic is unable to acquire services of OPES intermediary to achieve desired transformation.**
  - **A malicious OPES intermediary, serving as a DoS component, interrupts data flow between provider and consumer.**

- **SOLUTION:**
  - **Malicious data traffic emanating from particular suspect ports or IP addresses SHOULD be denied access to OPES intermediary.**
  - **Detection of malicious OPES intermediary, which has been successfully authenticated and authorized, is a hard problem which needs further study.**

End-point Entity Repudiates a Request

- **THREAT:**
  - **End-point entity that makes a certain request, by means of setting transformation rules, of an authorized OPES intermediary claims, later, that it did not make that request.**
- **EFFECT:**
  - **Entity that repudiates valid request for transformation by authorized OPES intermediary MAY be held liable for asked for changes to the data flow.**
- **SOLUTION:**
  - **Non-repudiation of requests for transformation of a data flow by an authorized OPES intermediary needs to be provided.**
  - **Use of digital signature to establish identity of requester.**
  - **Can be accomplished by use of private key for encrypting request for a transformation service.**

Conclusions and Next Steps

- <draft-srinivas-opes-threats-00.txt> discussed security threats that a data stream is exposed to owing to presence of an OPES intermediary (or call-out server).
- A more detailed investigation of the listed threats as well as solutions to mitigate their effects is needed.
- We would like to suggest this as a WG draft.