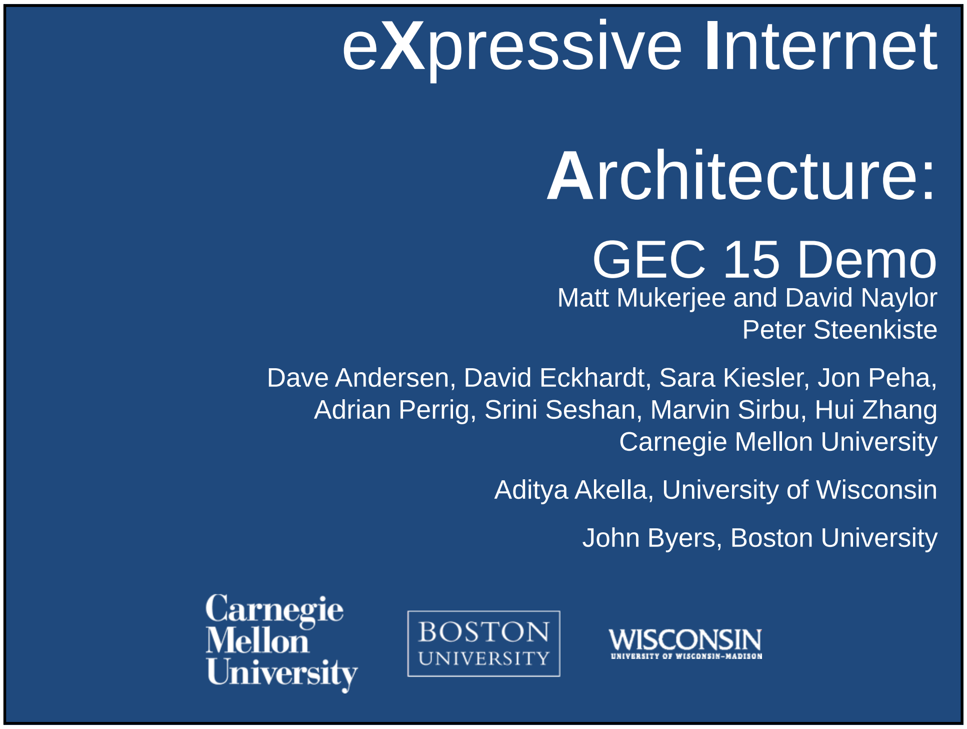


e**X**pressive **I**nternet **A**rchitecture:

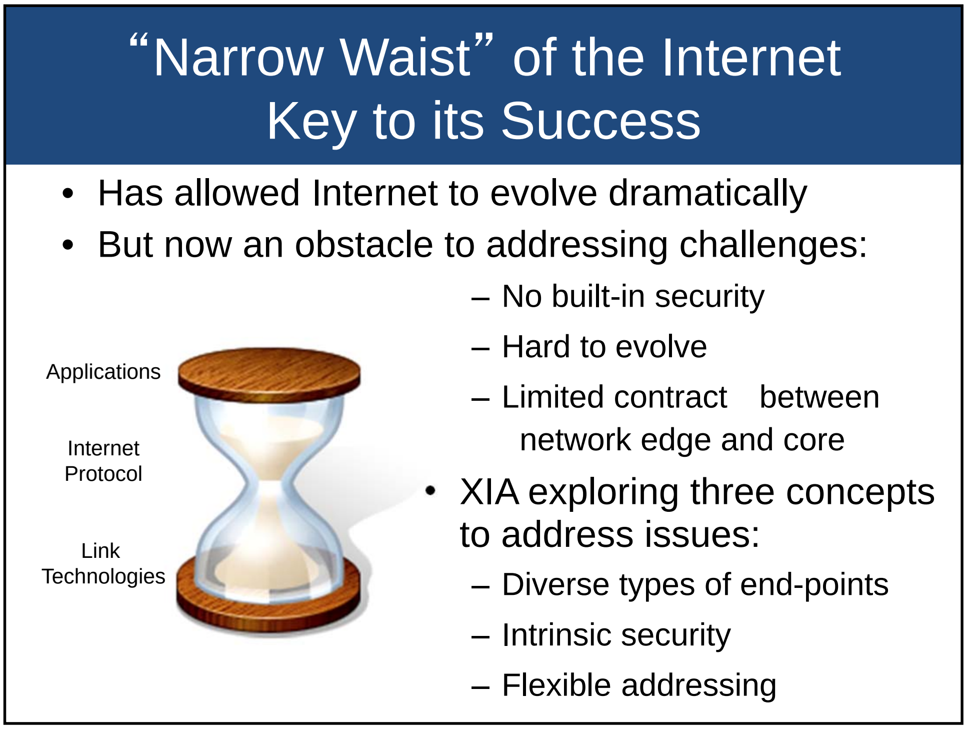
GEC 15 Demo

Matt Mukerjee and David Naylor
Peter Steenkiste

Dave Andersen, David Eckhardt, Sara Kiesler, Jon Peha,
Adrian Perrig, Srini Seshan, Marvin Sirbu, Hui Zhang
Carnegie Mellon University

Aditya Akella, University of Wisconsin

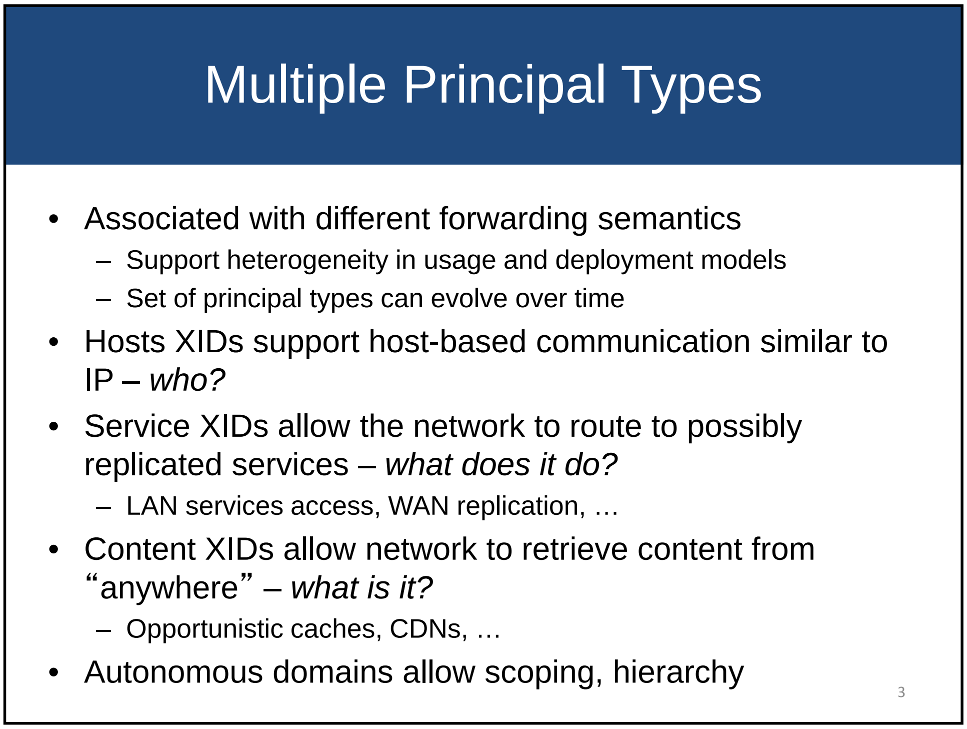
John Byers, Boston University



"Narrow Waist" of the Internet Key to its Success

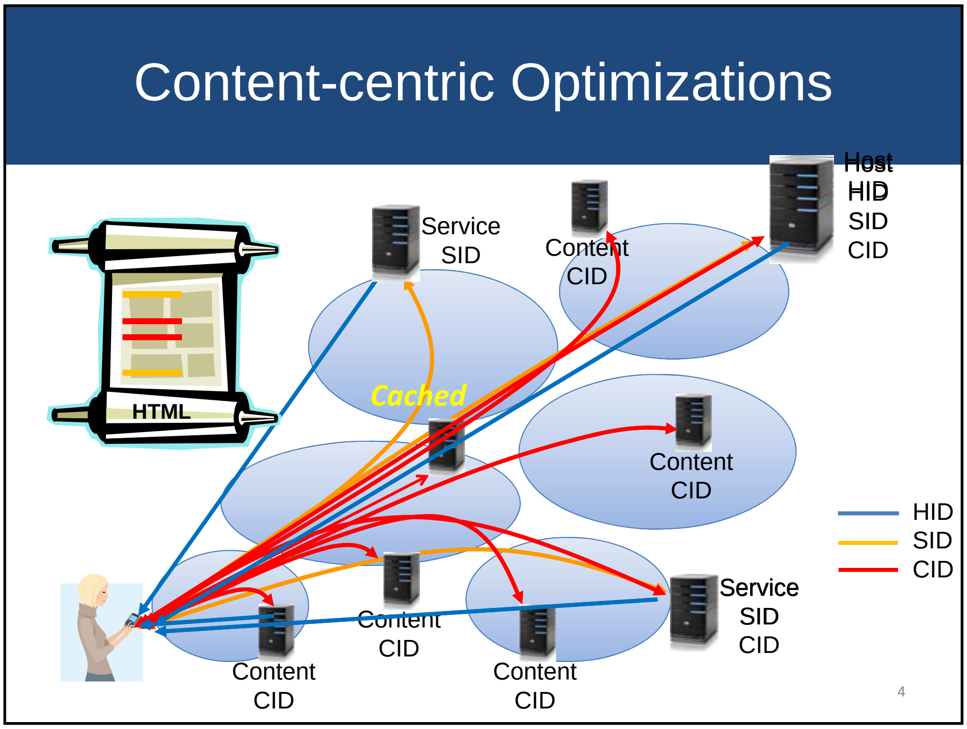
- Has allowed Internet to evolve dramatically
- But now an obstacle to addressing challenges:
  - No built-in security
  - Hard to evolve
  - Limited contract between network edge and core
- XIA exploring three concepts to address issues:
  - Diverse types of end-points
  - Intrinsic security
  - Flexible addressing

Applications
Internet Protocol
Link Technologies



Multiple Principal Types

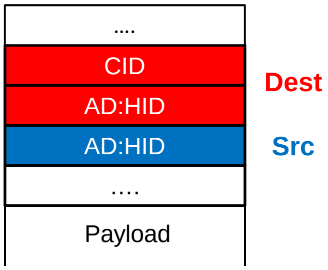
- Associated with different forwarding semantics
  - Support heterogeneity in usage and deployment models
  - Set of principal types can evolve over time
- Hosts XIDs support host-based communication similar to IP – *who?*
- Service XIDs allow the network to route to possibly replicated services – *what does it do?*
  - LAN services access, WAN replication, …
- Content XIDs allow network to retrieve content from “anywhere” – *what is it?*
  - Opportunistic caches, CDNs, …
- Autonomous domains allow scoping, hierarchy



Content-centric Optimizations

Supporting Evolvability

- New principal types must be deployed incrementally
  - No “flag” day
- Creates chicken and egg problem - what comes first: network support or use in applications
- Solution is to provide an *intent* and *fallback* address
  - Intent address allows in-network optimizations based on user intent
  - Fallback address is guaranteed to be reachable



....

CID

AD:HID

AD:HID

....

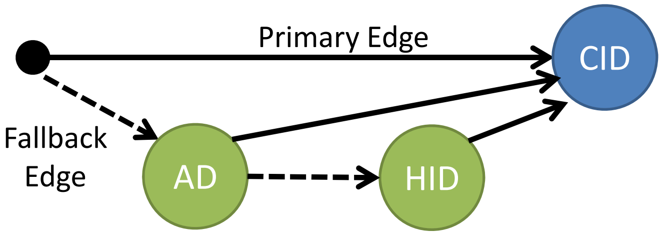
Payload

Dest

Src

Support for Fallbacks with DAG

- A node can have multiple outgoing edges



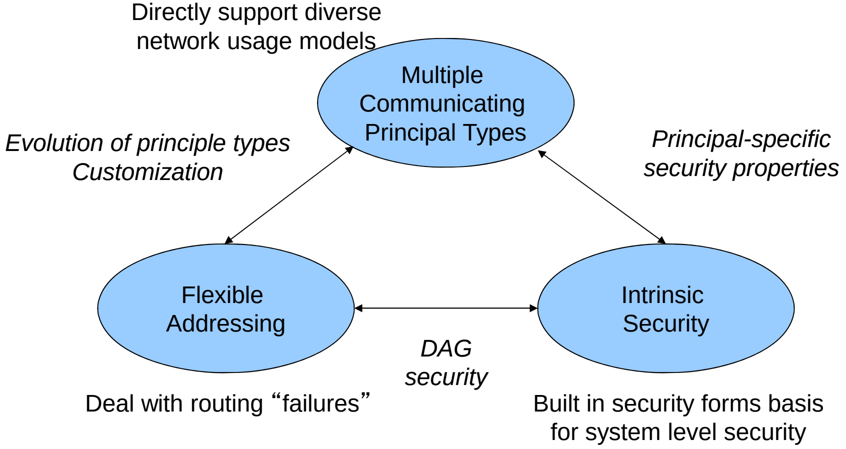
- Outgoing edges are prioritized
  - Forwarding to AD, HID is attempted only if forwarding to CID is not possible
- Also supports scoping, mobility, …

Intrinsic Security in XIA

- XIA uses self-certifying identifiers that guarantee security properties for communication operation
  - Host ID is a hash of its public key – accountability (AIP)
  - Content ID is a hash of the content – correctness
  - Does not rely on external configurations
- Intrinsic security is specific to the principal type
- Example: retrieve content using …
  - Content XID: content is correct
  - Service XID: the right service provided content
  - Host XID: content was delivered from right host

7

XIA Dataplane Concepts



Directly support diverse network usage models

Multiple Communicating Principal Types

Evolution of principle types Customization

Principal-specific security properties

Flexible Addressing

Intrinsic Security

DAG security

Deal with routing “failures”

Built in security forms basis for system level security

- Can be implemented in diverse ways
- Networks can implement different features

DEMO

4

Thing
s
Today

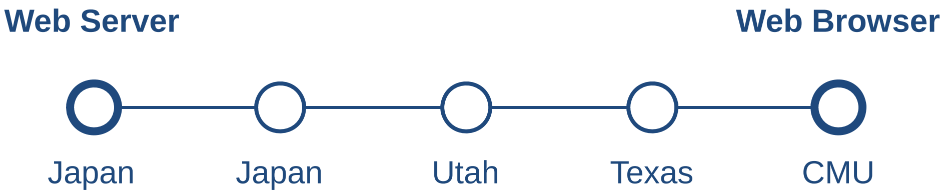
1 Evolvability

2 Intrinsic Security

3 Deployment over IP

4 Wireshark Plugin

Native XIA Applications



Web Server

Web Browser

Japan

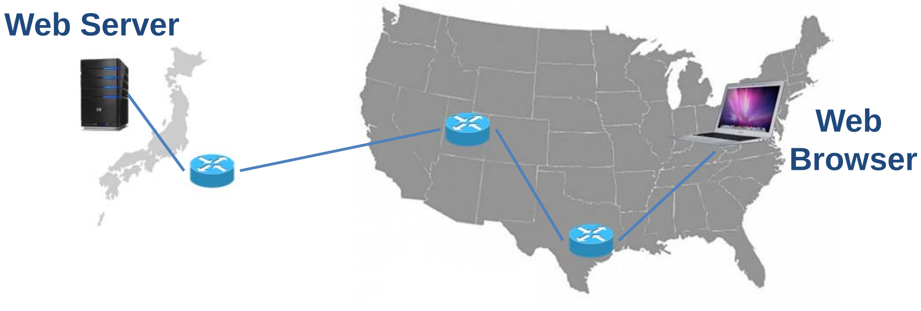
Japan

Utah

Texas

CMU

Topology



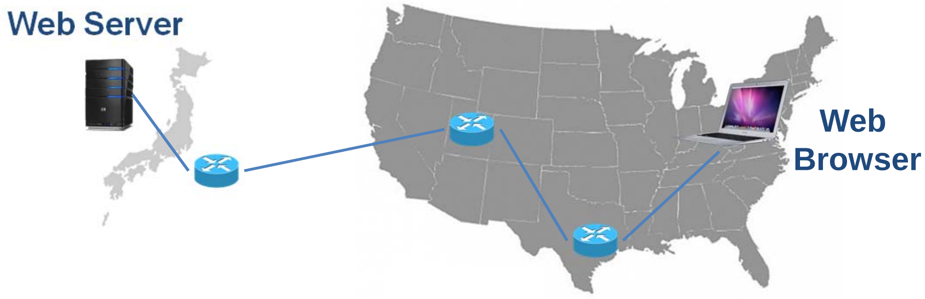
Web Server

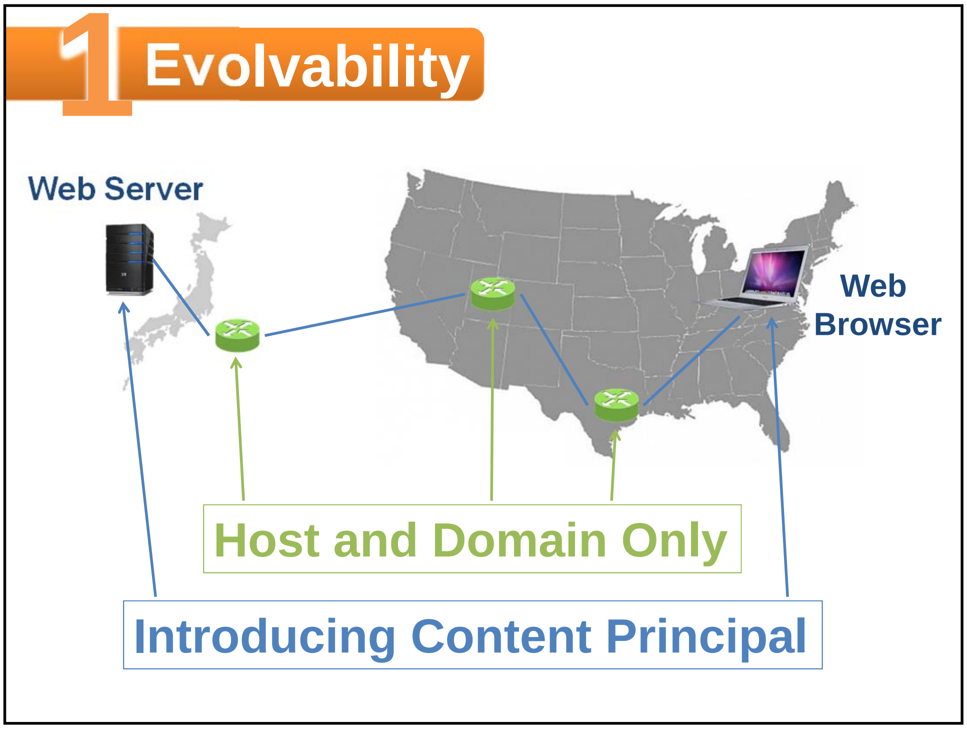
Web Browser

Native XIA Applications

1 Evolvability

1 Evolvability





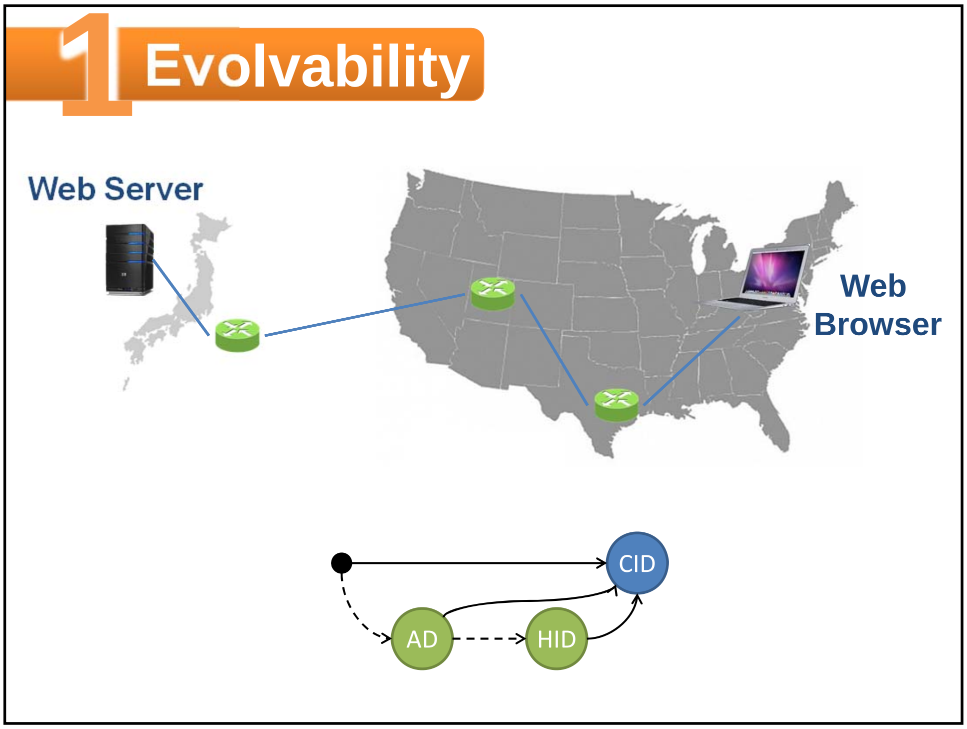
1 Evolvability

Web Server

Web Browser

Host and Domain Only

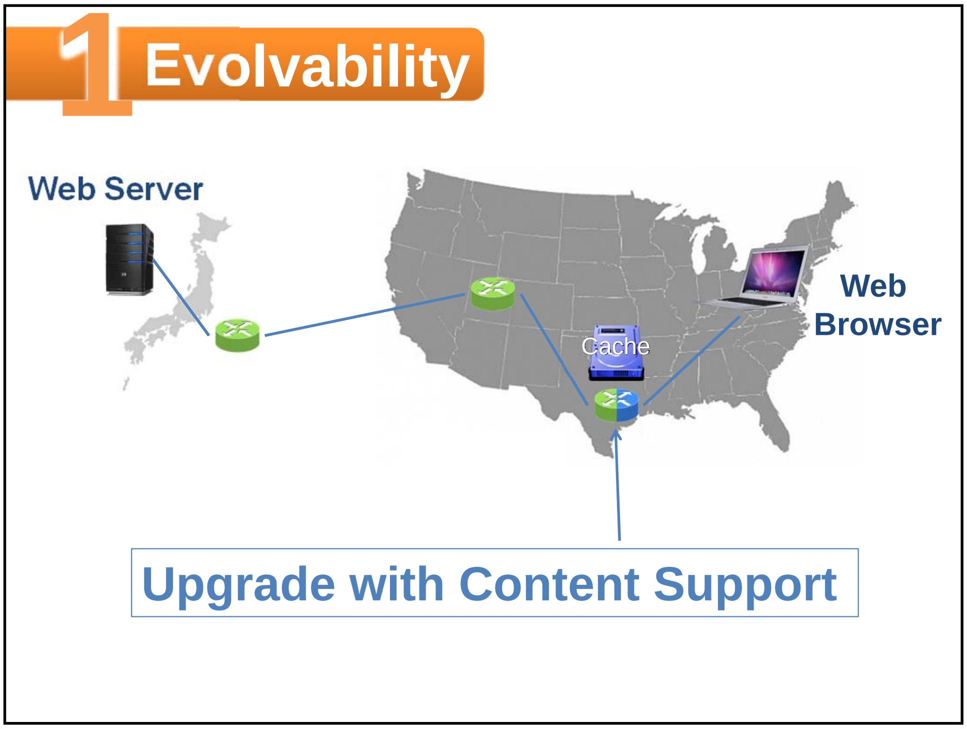
Introducing Content Principal



1 Evolvability

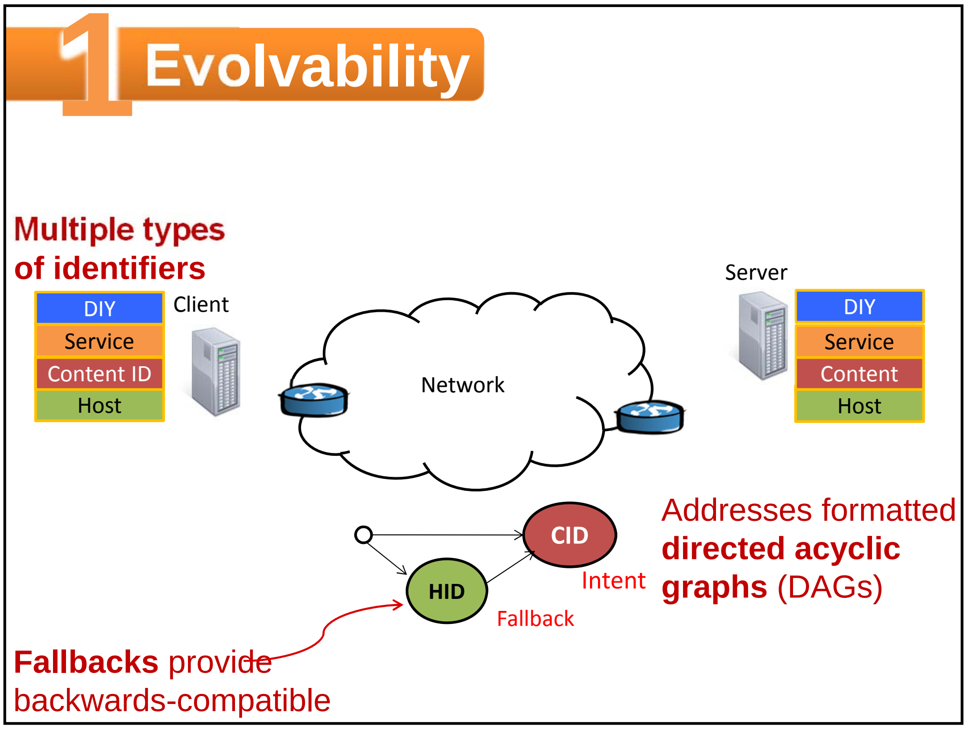
Web Server

Web Browser



1 Evolvability

Upgrade with Content Support

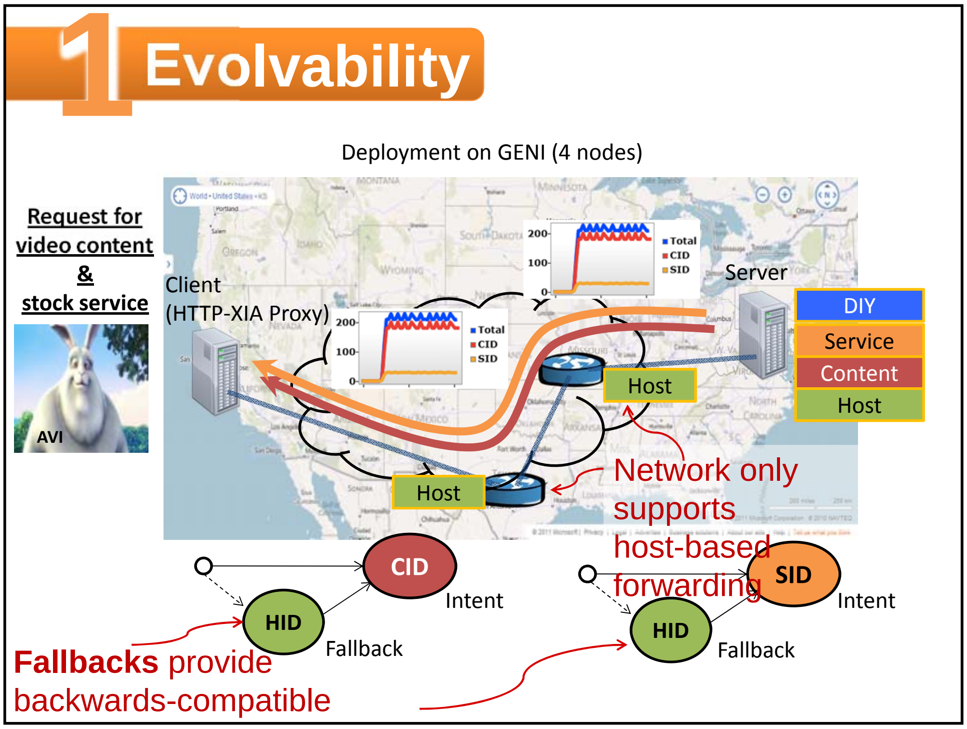


1 Evolvability

Multiple types of identifiers

Addresses formatted **directed acyclic graphs** (DAGs)

Fallbacks provide backwards-compatible



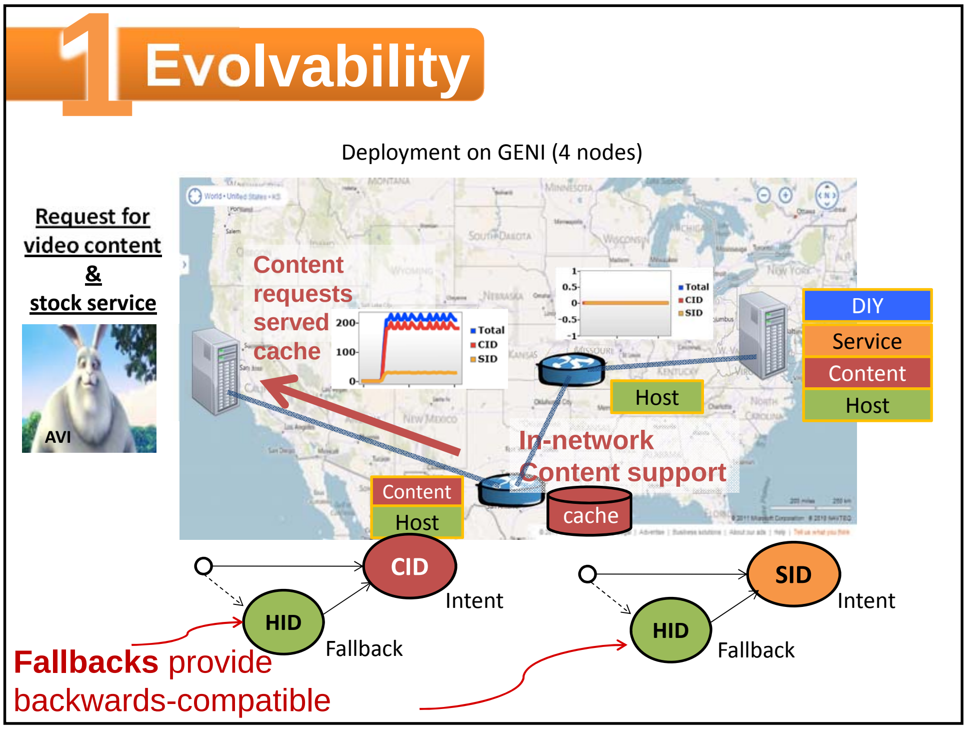
1 Evolvability

Deployment on GENI (4 nodes)

Request for video content & stock service

Network only supports host-based forwarding

Fallbacks provide backwards-compatible



1 Evolvability

Deployment on GENI (4 nodes)

Request for video content & stock service

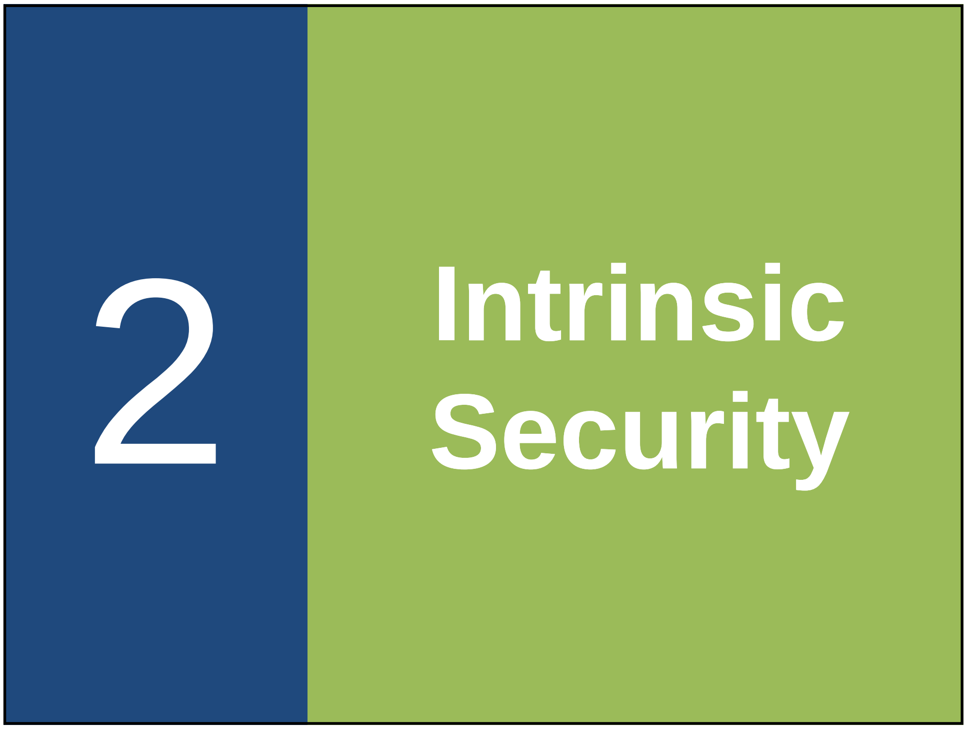
Content requests served cache

In-network Content support

Fallbacks provide backwards-compatible

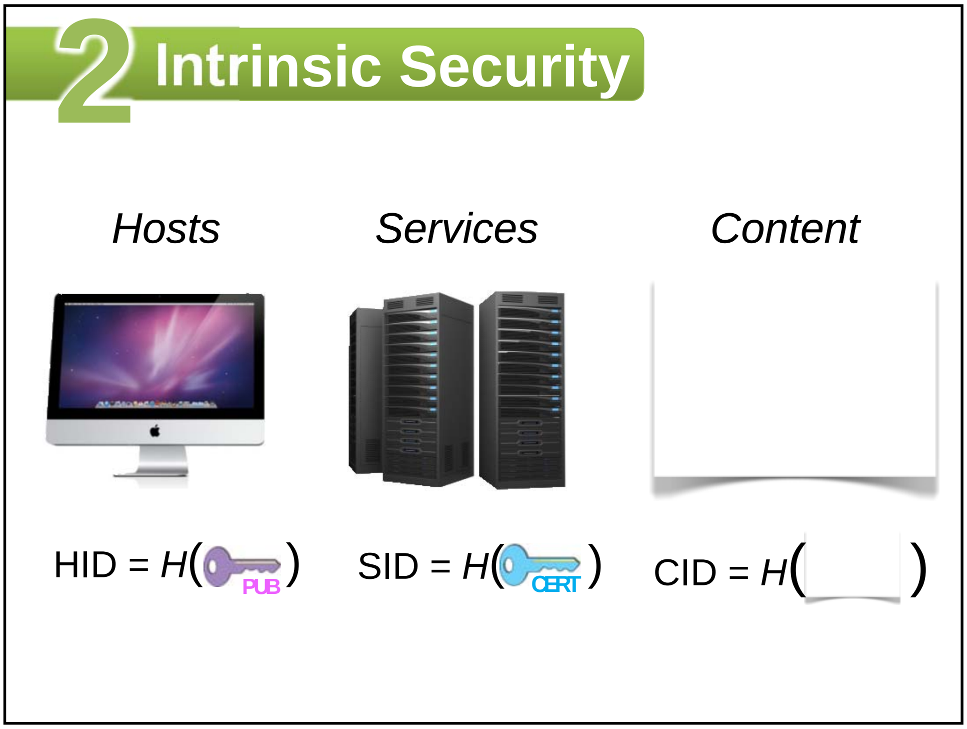
1

Evolvability



2

Intrinsic Security



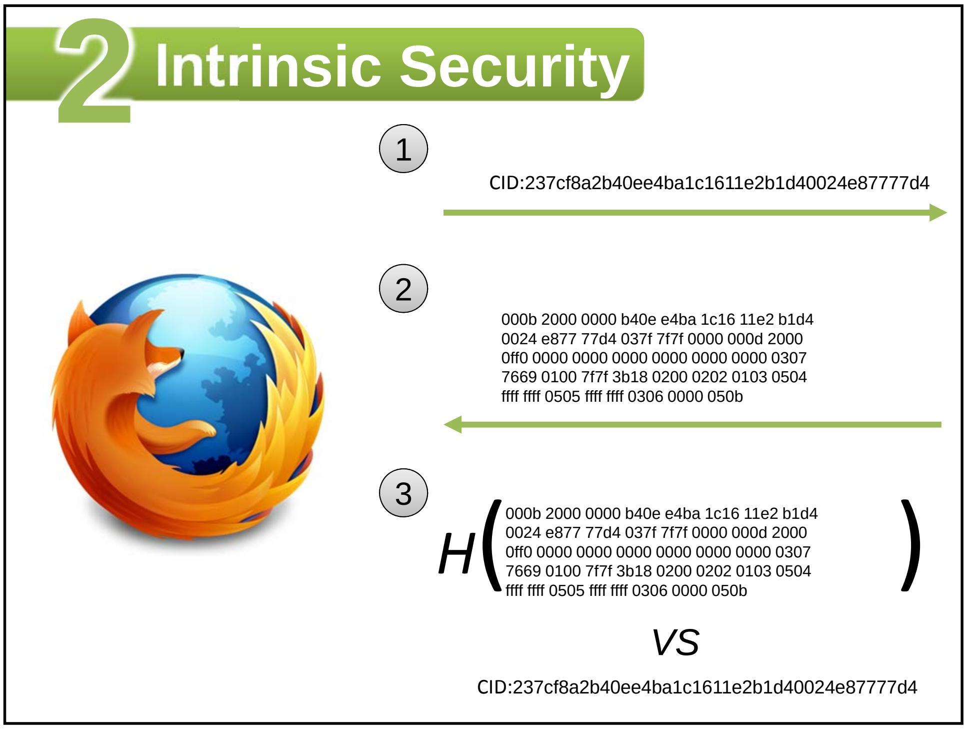
2 Intrinsic Security

Hosts *Services* *Content*

HID = *H*(PUB)

SID = *H*(CERT)

CID = *H*( )



2 Intrinsic Security

1

CID:237cf8a2b40ee4ba1c1611e2b1d40024e87777d4

2

```
000b 2000 0000 b40e e4ba 1c16 11e2 b1d4
0024 e877 77d4 037f 7f7f 0000 000d 2000
0ff0 0000 0000 0000 0000 0000 0000 0307
7669 0100 7f7f 3b18 0200 0202 0103 0504
ffff ffff 0505 ffff ffff 0306 0000 050b
```

3

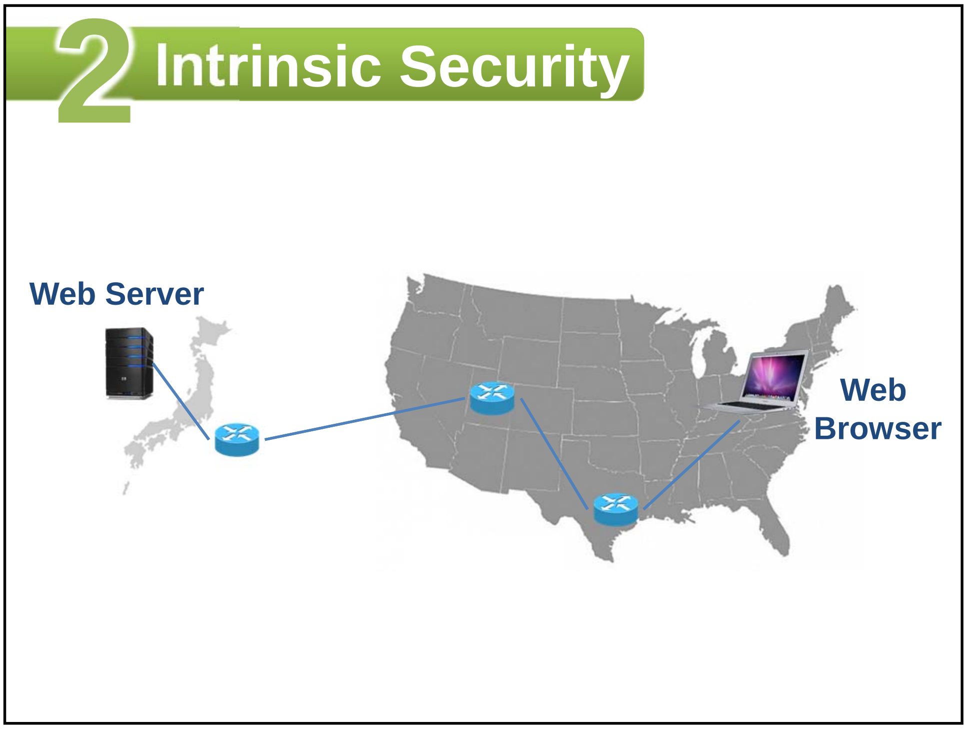
H(

```
000b 2000 0000 b40e e4ba 1c16 11e2 b1d4
0024 e877 77d4 037f 7f7f 0000 000d 2000
0ff0 0000 0000 0000 0000 0000 0000 0307
7669 0100 7f7f 3b18 0200 0202 0103 0504
ffff ffff 0505 ffff ffff 0306 0000 050b
```

)

VS

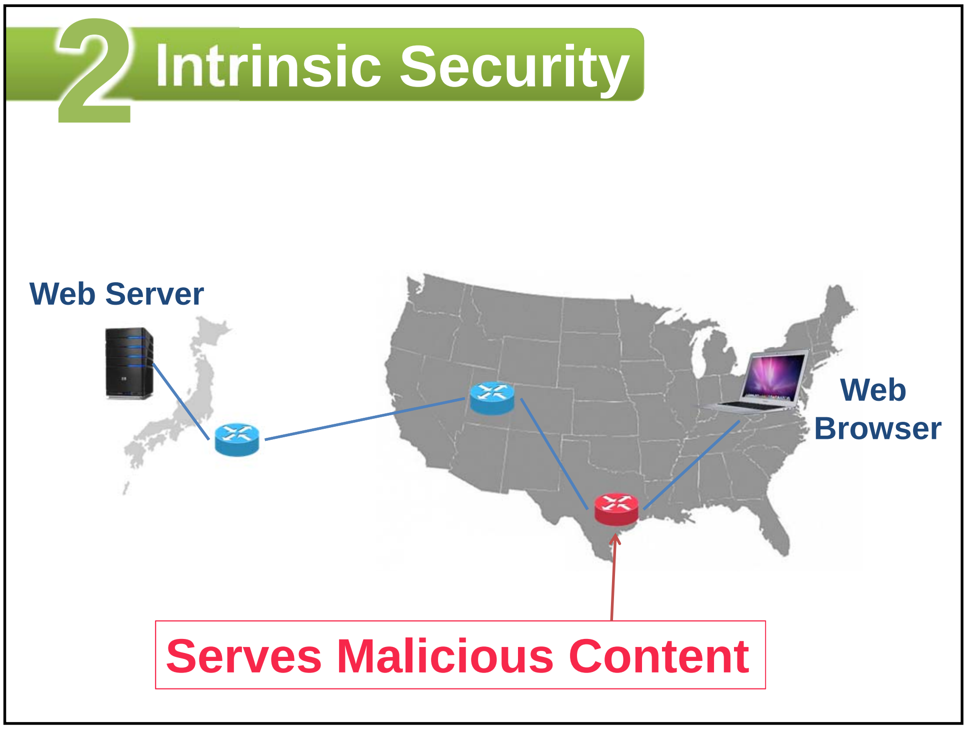
CID:237cf8a2b40ee4ba1c1611e2b1d40024e87777d4



2 Intrinsic Security

Web Server

Web Browser

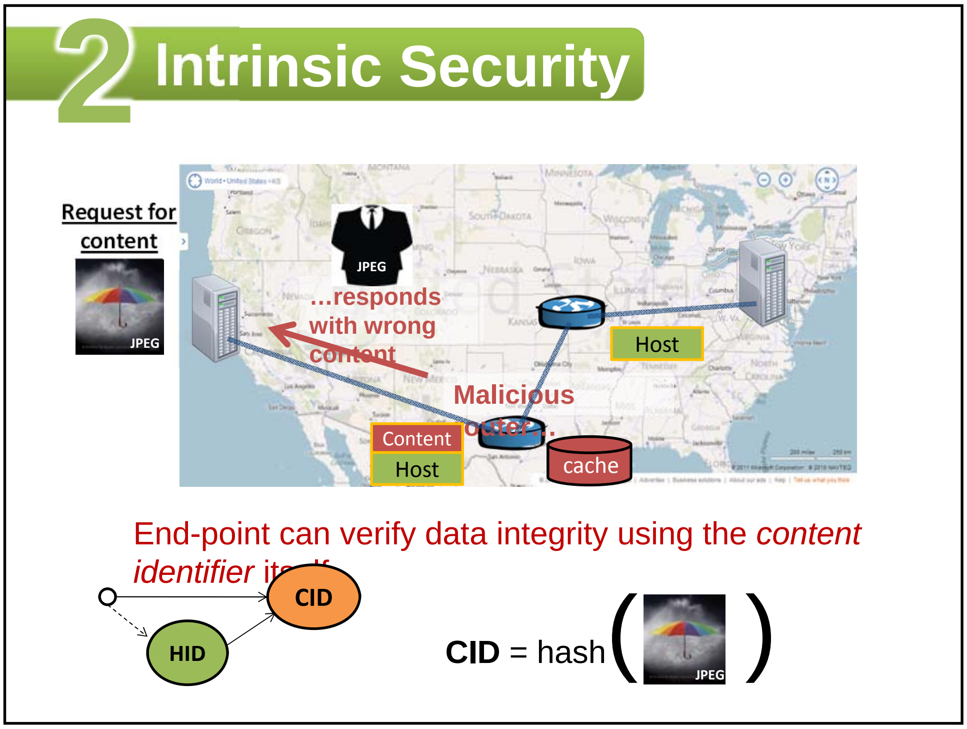


2 Intrinsic Security

Web Server

Web Browser

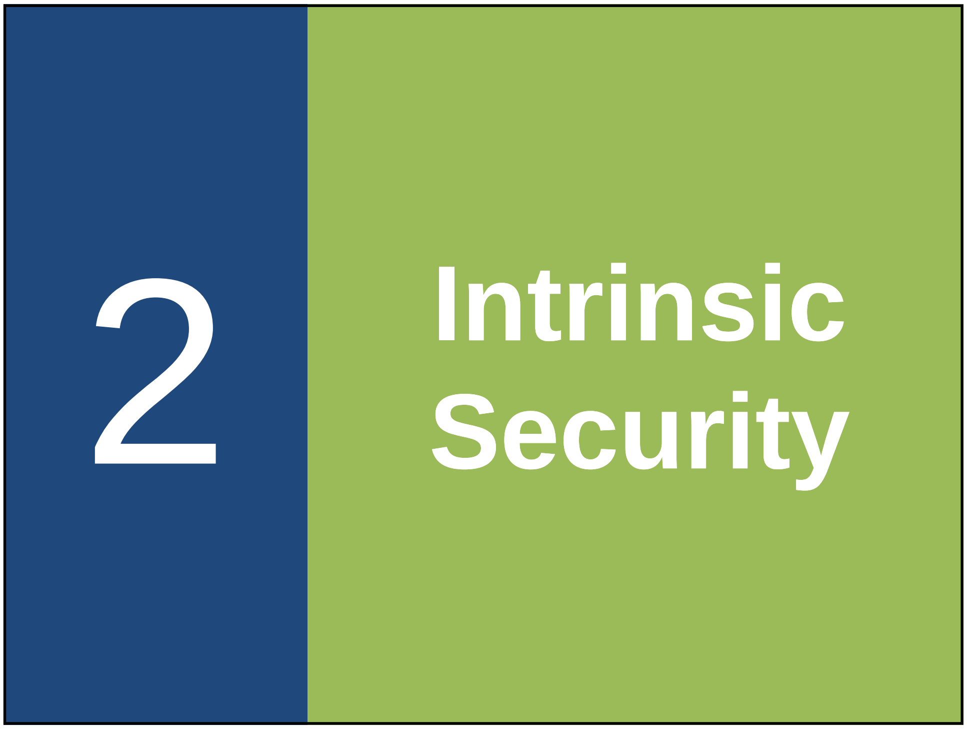
Serves Malicious Content



2 Intrinsic Security

End-point can verify data integrity using the *content identifier itself*

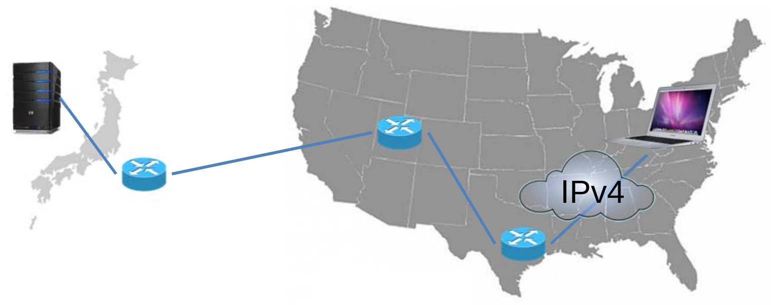
CID = hash(JPEG)

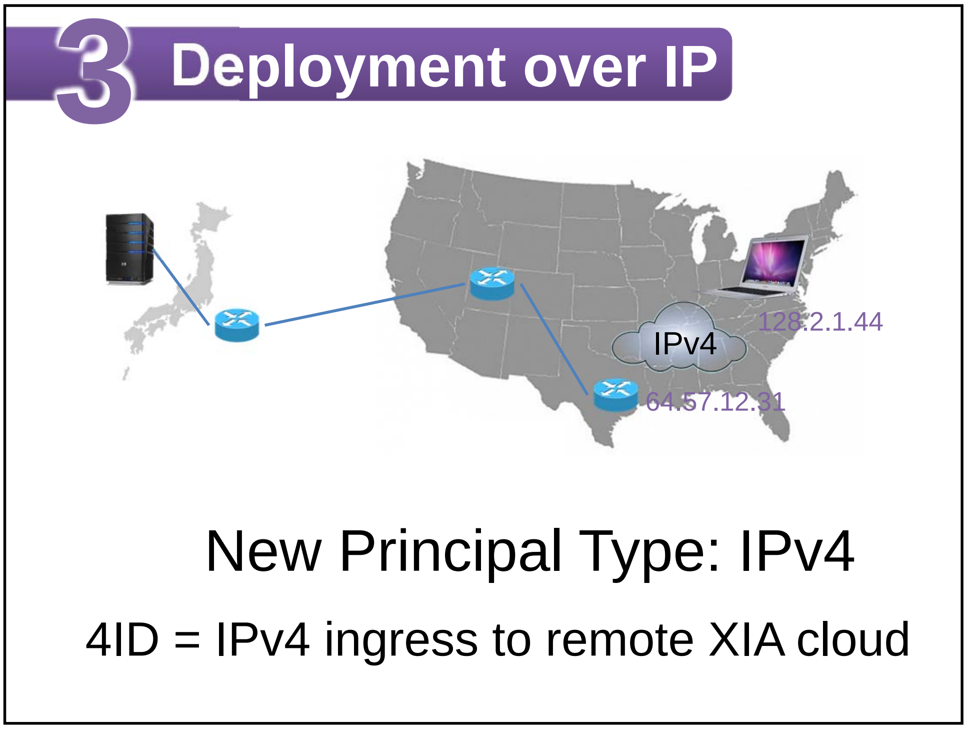


2 Intrinsic Security

3 Deployment over IP

3 Deployment over IP

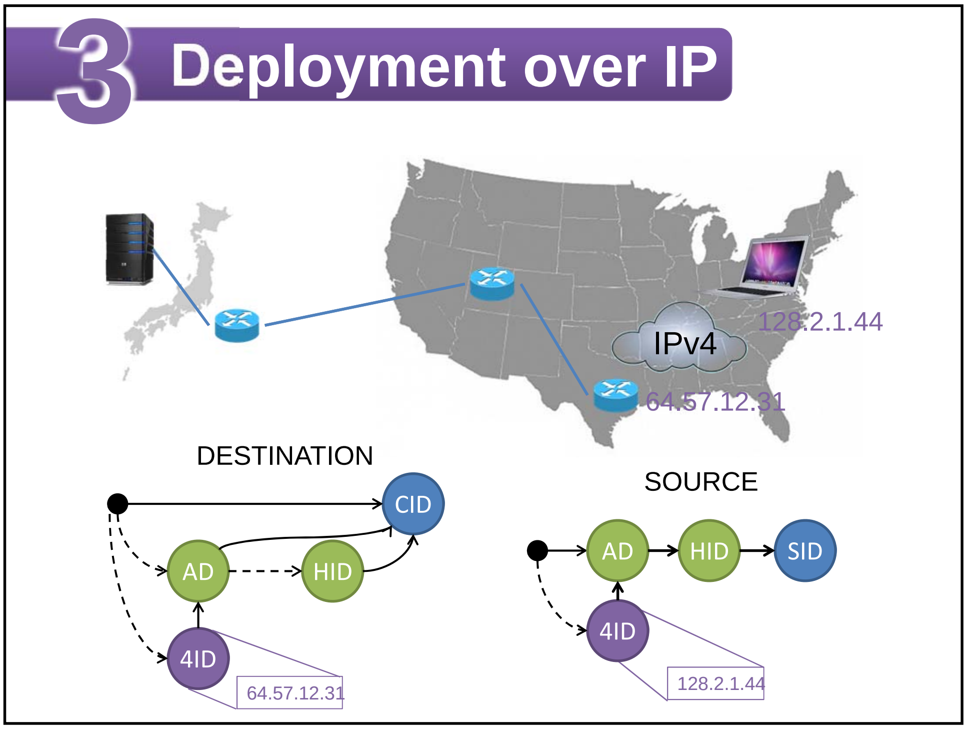




3 Deployment over IP

New Principal Type: IPv4

4ID = IPv4 ingress to remote XIA cloud



3 Deployment over IP

3

Deployment over IP

4

Wireshark Plugin

4 Wireshark Plugin

Debug your XIA network

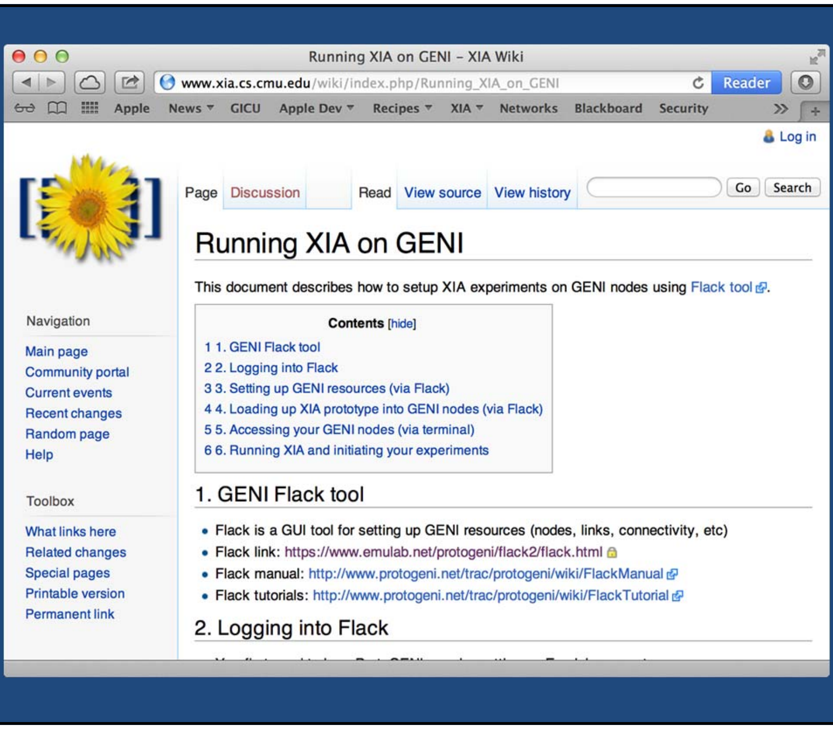
4 Wireshark Plugin

One more thing…

XIA Prototype:
DIY!

Public Release

- Tarball
- Github
- VM



Running XIA on GENI

This document describes how to setup XIA experiments on GENI nodes using Flack tool.

Navigation

- Main page
- Community portal
- Current events
- Recent changes
- Random page
- Help

Toolbox

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

Contents [hide]

1. GENI Flack tool

- Flack is a GUI tool for setting up GENI resources (nodes, links, connectivity, etc)
- Flack link: https://www.emulab.net/protogeni/flack2/flack.html
- Flack manual: http://www.protogeni.net/trac/protogeni/wiki/FlackManual
- Flack tutorials: http://www.protogeni.net/trac/protogeni/wiki/FlackTutorial

2. Logging into Flack

eXpressive Internet Architecture:

GEC 15 Demo

www.cs.cmu.edu/~xia

Carnegie Mellon University

BOSTON UNIVERSITY

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON