Identity and Location: implications for Security, Privacy and Resilience

Saleem Bhatti
School of Computer Science
University of St Andrews

Dagstuhl Seminar 15151
10 Apr 2015
Caveat

• I have 15 mins only ... so ...

• Highlight high-level ideas:
  • some examples from today’s world.

• Make the case that identity and location need to be considered explicitly in the design and implementation of security, privacy and resilience mechanisms:
  • has impact on users, applications and services.
  • needs to be considered at system design overall.
Scope and Definitions

• An **identity**:
  • a “name” (set of bits) that (uniquely) labels some entity (a device, a user, a host/node, etc.)

• A **locator**:
  • a “name” (set of bits) that labels allows the topological and/or geographical and/or physical position of an entity

• While these could be considered technical issues only, some form of **identity** and **location** might be used in in policies, SLAs, system configurations, etc.
Identity and Location

- Identity is used for many protocols, services and applications:
  - identity required to access services
  - identity used for authentication and access control
- Already well-known problems on uses of identity and location, e.g.:
  - identity theft
  - location tracking
- Explicit identity and location may be required for operation of applications, services and systems.
- Explicit Identity and location may offer new opportunities for security, privacy and resilience.
Example: mobile phone service

- Identity:
  - required to uniquely identify subscribers
- Location:
  - required to route calls correctly
- Without explicit use of identity and location, the mobile phone service would not function.
- (Also, smartphones have GPS.)
- However, it does mean that there is information about exactly where you are!
- This is largely understood and accepted.
Identity

• End-to-end integrity of services:
  • end-to-end state
  • invariant / stable value to allow protocols to maintain a session or connection
 • Can use middleboxes:
  • additional complexity
  • additional entity that needs to be trusted
  • additional point of attack for disrupting communication
• Trade-off:
  • service vs. visibility of identity
IP addresses

- Provide both identity and location of a host:
  - overloaded semantics
- End-to-end state is tied to location:
  - mobility is harder
  - multiple connectivity is harder
  - packet-level security is bound to a location
- Can use middleboxes:
  - usual problem of an additional entity
- Trust boundary
New namespaces, separate semantics

- Semantic overload of IP address:
  - **locator** semantics + **identifier** semantics
  - ease implementation of multi-homing, mobility, etc …

- This is a well-known problem:
  - RFC4984, IAB (2007)
  - RFC2101, IAB (1997)
  - **IEN1** (1977)

- Many “ID/Locator separation” solutions proposed:
  - HIP, LISP, SHIM6, SixOne – re-use of IP address
  - **ILNP** – deprecates use of IP addresses:
    - RFC 6740-6748 (Experimental, IRTF RRG)
“IP addresses considered harmful”

- “IP addresses considered harmful”
  Brian E. Carpenter
  ACM SIGCOMM CCR, vol. 44, issue 2, Apr 2014
  http://dl.acm.org/citation.cfm?id=2602215
  http://dx.doi.org/10.1145/2602204.2602215

- Abstract
  “This note describes how the Internet has got itself into deep trouble by over-reliance on IP addresses and discusses some possible ways forward.”
ILNP: transport layer state example

A = IP address
P = port number

At X:

At Y:

L = Locator
I = (Node) Identifier
P = port number

At X:

At Y:
Mobility: hard handoff

- Hard handoff model used by MIP
- ILNP supports hard handoff also:
  - move from one cell to another
  - drop locator (prefix) $L_1$, use locator (prefix) $L_2$
Mobility: soft handoff

- ILNP support soft handoff (similar concept to CDMA)
- Both old locator ($L_1$) and new locator ($L_2$) used in overlap region
- Mobile host is multihomed during handoff
Inter-Datacentre Movement for VM

1. $[I_V, L_1] \rightarrow [V, H_1]$ from site network $L_1$
2. $[I_V, L_2] \rightarrow [V, H_2]$ from site network $L_2$

External link 1, $L_1$
External link 2, $L_2$

SBR1
SBR2

Internet

CN

A address (IP address)
CN correspondent node
H host
I identifier
L locator
SBR site border router
V virtual machine image

(C) Saleem N. Bhatti, 10 Apr 2015
IPsec

- Packet-level security for IP.
- IP addresses form part of end-to-end session security association (SA).
- If address changes, SA is invalid.
- If an identity is used, end-to-end state is invariant:
  - dynamic binding to location
  - update to location needs to be protected but can be signalled end-to-end
Summary: Identity and Location

• Sensitive information:
  • may expose privacy and security constraints.

• Opportunity:
  • explicit recognition of identity and location could be used for enhancing security and resilience.

• ILNP applies this to the network layer:
  • higher layer application of similar principles is possible and could lead to opportunities for enhanced security, privacy and resilience.