Countering Phishing Threats with Trust-by-Wire in Packet-Switched IP Networks

Stephan Kubisch, Harald Widiger, Peter Danielis,
Jens Schulz, Dirk Timmermann

stephan.kubisch@uni-rostock.de

University of Rostock

Institute of Applied Microelectronics and Computer Engineering

Thomas Bahls, Daniel Duchow

Nokia Siemens Networks

Broadband Access Division
Greifswald, Germany

4th SSN @ 22nd IEEE IPDPS, Miami, FL, USA, April 18, 2008

Outline

1. **Introduction & Motivation**
2. The General IPclip Mechanism
3. Anti-Phishing Framework
4. Summary

1. Introduction & Motivation

- Internet = open mass-medium
- Ubiquitous, cheap, comfortable …
- But what about phishing, spam, malware, privacy issues...?

- What can be done?
  - Sensitize the people
  - Use anti-x tools for protection
  - Analyze anomalies
  - Detect & trace threats

→ Make the Internet more secure!

We do have a security problem!

Internet lacks trustworthiness!

1. Introduction & Motivation

Public Switched Telephone Network vs. Internet

Public Switched Telephone Network

- Line-switched
- Call number identifies access line and an address
- Direct interrelationship with location information : Trust-by-Wire!

Internet

- Packet-switched
- IP addresses are ambiguous and prone to manipulation!
- No interrelation with location information : No Trust-by-Wire!
- Apply Trust-by-Authentication to provide user trustworthiness

Most users only believe their eyes!
→ How can true mutual trust be realized?

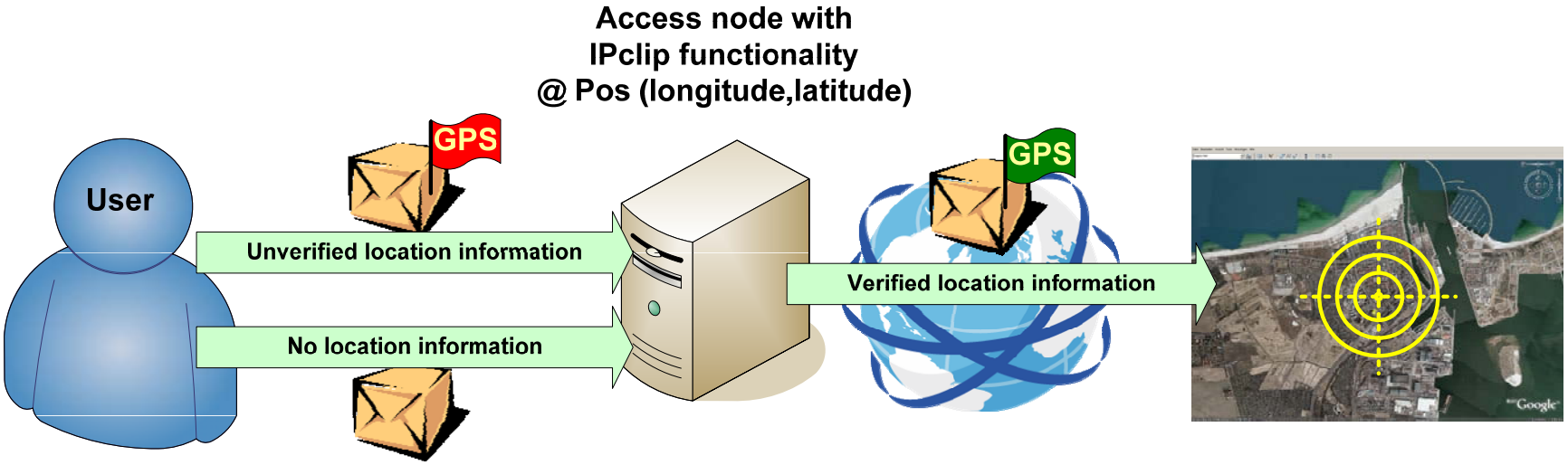
Outline

1. Introduction & Motivation
2. **The General IPclip Mechanism**
3. Anti-Phishing Framework
4. Summary

2. The General IPclip Mechanism

IPclip is used to provide TBW in IP networks

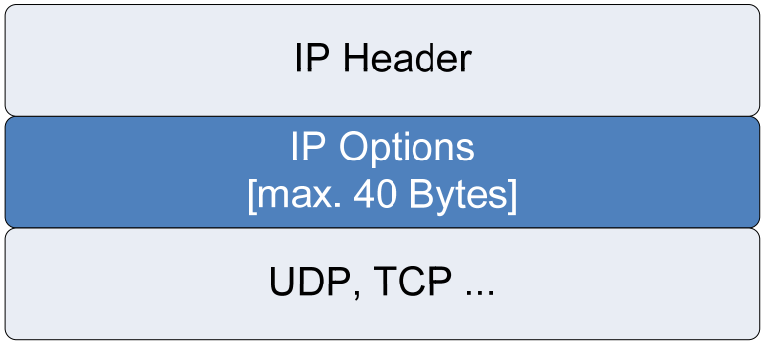
- IPclip = IP Calling Line Identification Presentation
- Location information (LI) is added to each IP packet as **IP option** (GPS coordinates for example)
  - …either by the user or by IPclip, but always verified by IPclip



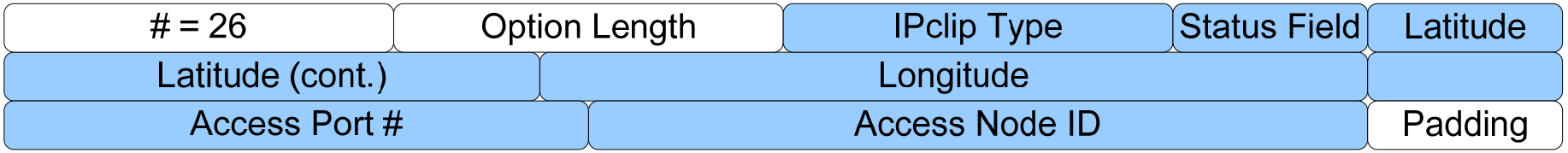
2. The General IPclip Mechanism

What kind of location information do we use?

- IPv4 header allows use of IP options
- Type-length-value structure



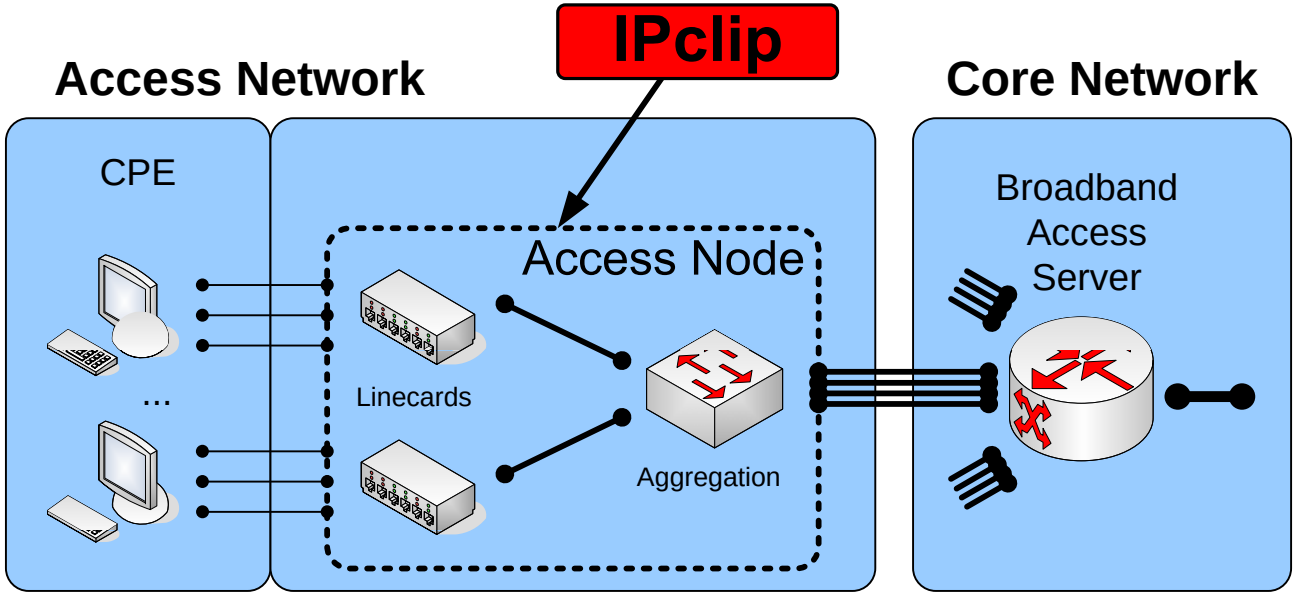
- IPclip Option (light blue) = value of an IP option
- Example: GPS coordinates + port ID + node ID



2. The General IPclip Mechanism

Access network most reasonable place for IPclip!

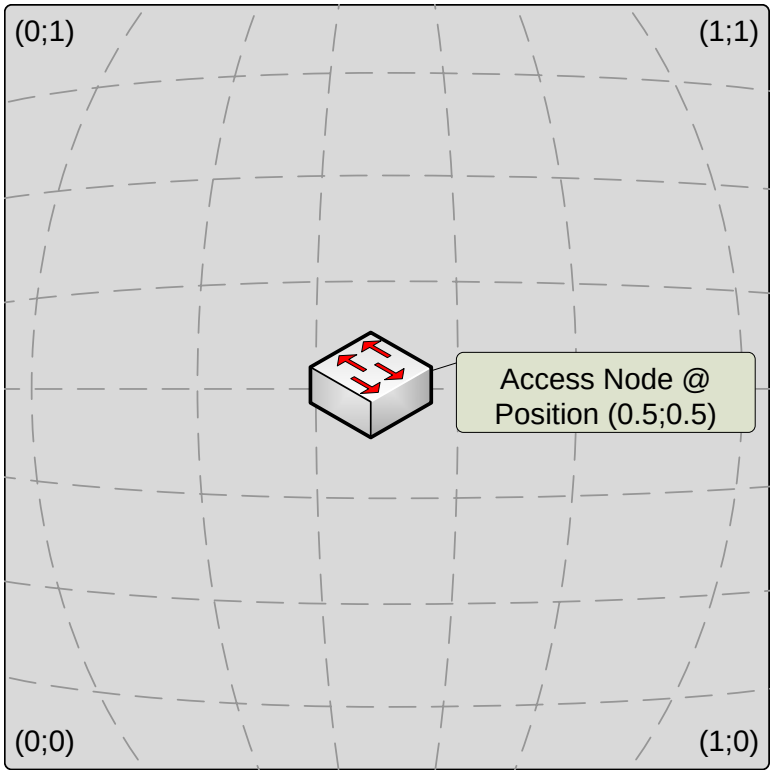
- Access node is the 1st trustworthy network element
  - Place to verify user provided LI
  - Access port + access node ID as complementary information



2. The General IPclip Mechanism

IPclip verifies location information to ensure trustworthiness.

- LI is trustworthy if within access node's ***subscriber catchment area***



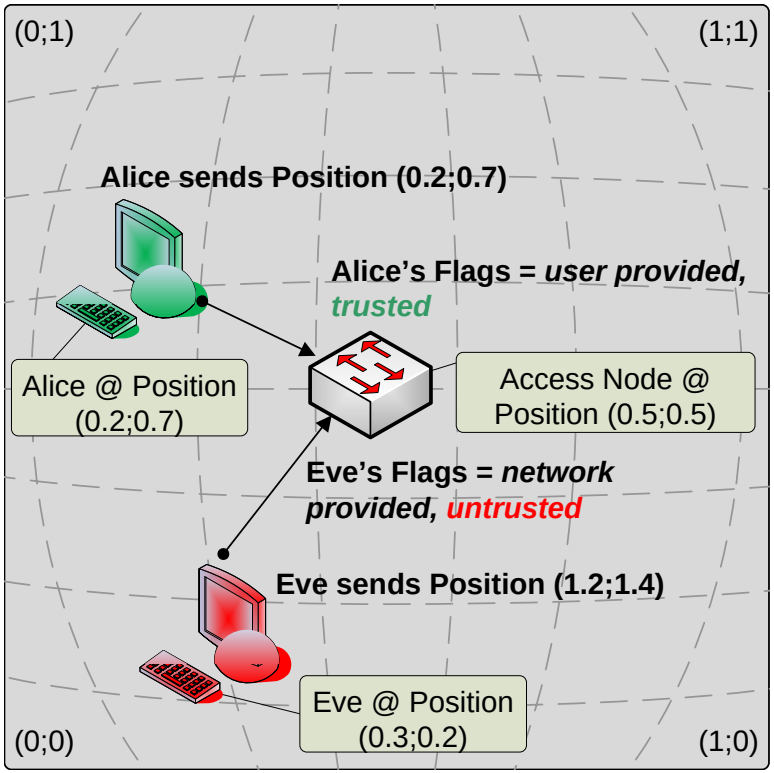
Access node's subscriber catchment area with normalized coords'

2. The General IPclip Mechanism

IPclip verifies location information to ensure trustworthiness.

- IPclip sets status flags on the access node depending on the verification result

Source/Trust	Interpretation	Status Flags
User provided/ untrusted	User LI incorrect.	00
User provided/ trusted	User LI correct.	01
Network provided/ untrusted	User LI incorrect and replaced.	10
Network provided/ trusted	No user LI. Access node LI added.	11



Access node's subscriber catchment area with normalized coords'

Outline

1. Introduction & Motivation
2. The General IPclip Mechanism
3. **Anti-Phishing Framework**
4. Summary

3. Anti-Phishing Framework

Basic steps within the framework

a. A trustworthy institution (bank) publishes an ***IPclip signature***.
   - Accessible via public a data base server

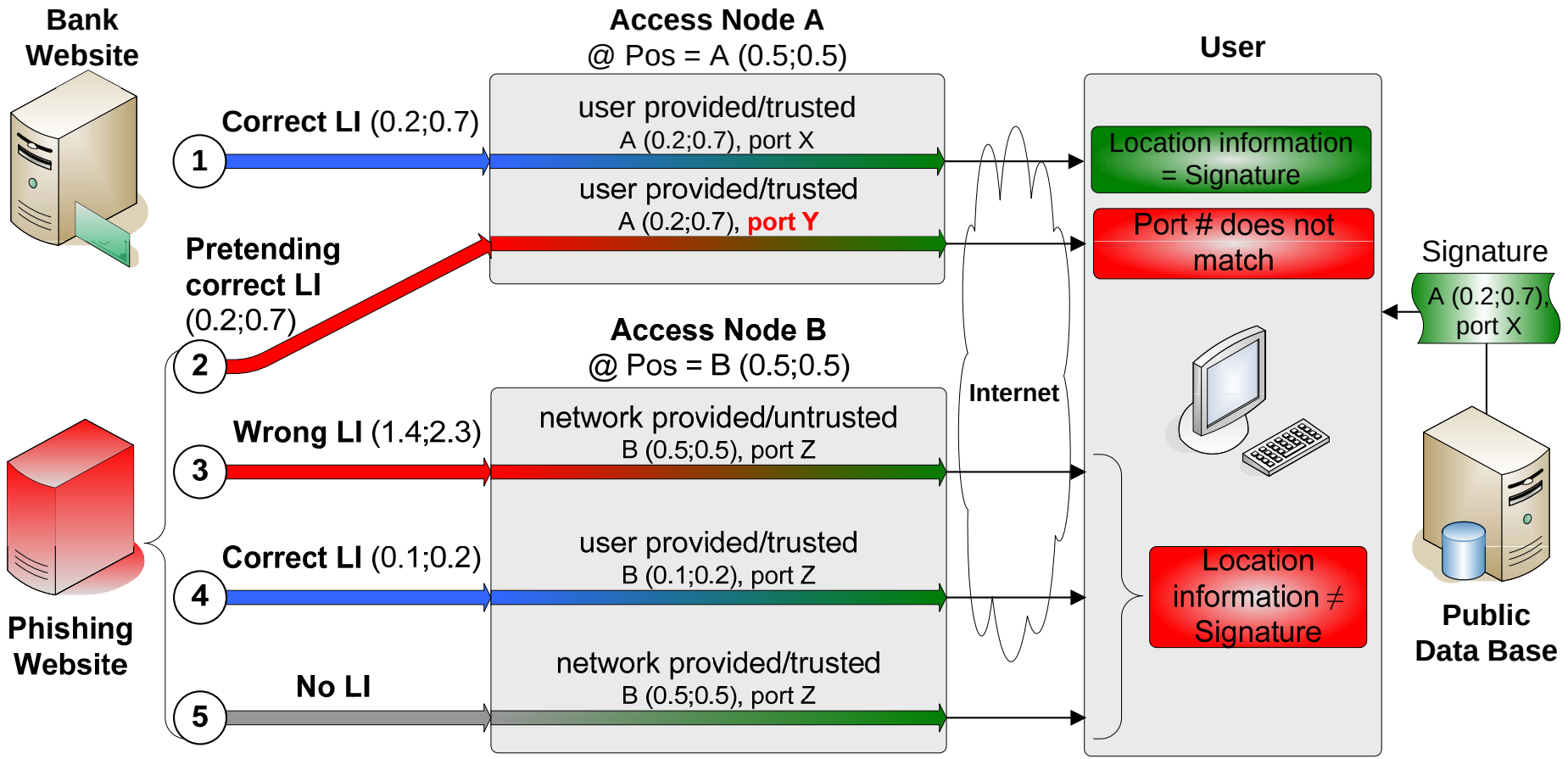
b. The bank provides IPclip options in outgoing IP traffic.

c. IPclip on the access node verifies LI.
   - Additionally, access port number and access node ID are added.

d. User ***compares*** public signature with verified IPclip LI.
   - If both match, everything is fine…

3. Anti-Phishing Framework

Provision and verification of location information



3. Anti-Phishing Framework

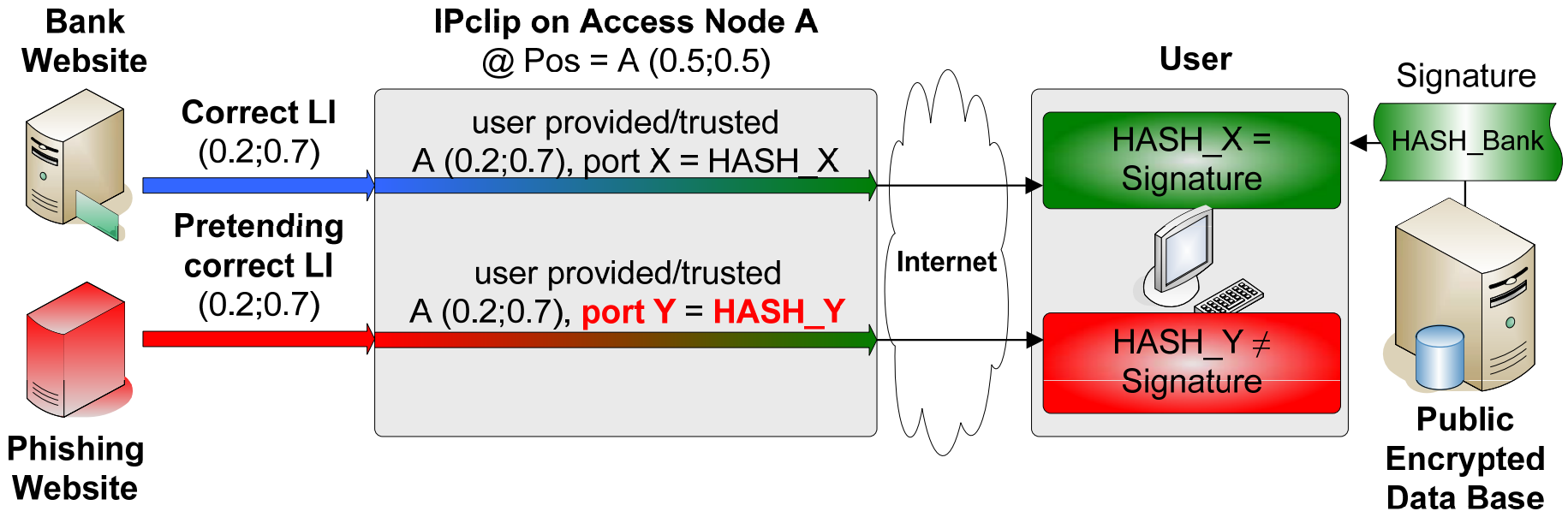
Requirements and constraints for this use case

- The operator of a trustworthy website should always provide LI in outgoing IP packets!
- Fully IPclip-terminated domain, e.g., a self-contained provider network
  - IPclip is mandatory for all access nodes!
- IPclip-capable IP stack in relevant network devices
  - To understand IPclip options and LI
  - Other devices just forward IP options!
- Privacy issues!
  - See next slide…

3. Anti-Phishing Framework

Privacy issues – revelation of sensitive location information?

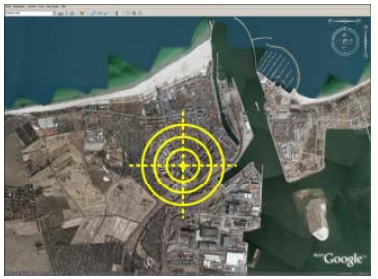
- Use an encrypted LI, e.g., by hashing!
  - Encryption is *only* done on the access node



3. Anti-Phishing Framework

Advantages?

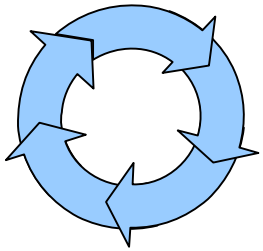
- Detection and Prevention of phishing attempts by comparison of the IPclip LI with a public signature
  - True mutual trust between user and online service instead of unidirectional trust relationship
- IPclip LI is outside a phisher's sphere
  - Cannot be manipulated
- Secondary: Tracing the origin of the phishing attempt using the IPclip LI (without encryption)



Outline

1. Introduction & Motivation
2. The General IPclip Mechanism
3. Anti-Phishing Framework
4. **Summary**

4. Summary



- **Location information is added to each IP packet**
- **Providing a location reference to the sender**

- **Trustworthy institutions provide signatures to be compared with location information inside IP**

- **Detection and prevention of phishing attempts**
- **True mutual trust relationship**

- **Allows for tracing the origin of phishing attempts**

- **More use cases exist…**
  (e.g., VoIP Emergency Calls, Spam Detection)

Thank you! Any questions?

stephan.kubisch@uni-rostock.de
http://www.imd.uni-rostock.de/networking