Experimental Results of Covert Channel Limitation in One-Way Communication Systems

Nick Ogurtsov, Hilarie Orman, Richard Schroeppel, Sean O'Malley, Oliver Spatscheck

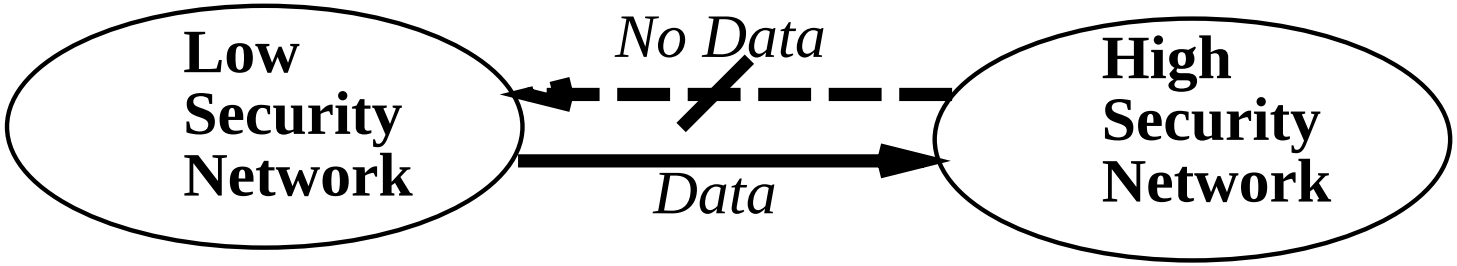
University of Arizona

Outline

- Introduction
- Simple Solutions
- Previously Proposed Protocols
- Quantized Pump
- Summary

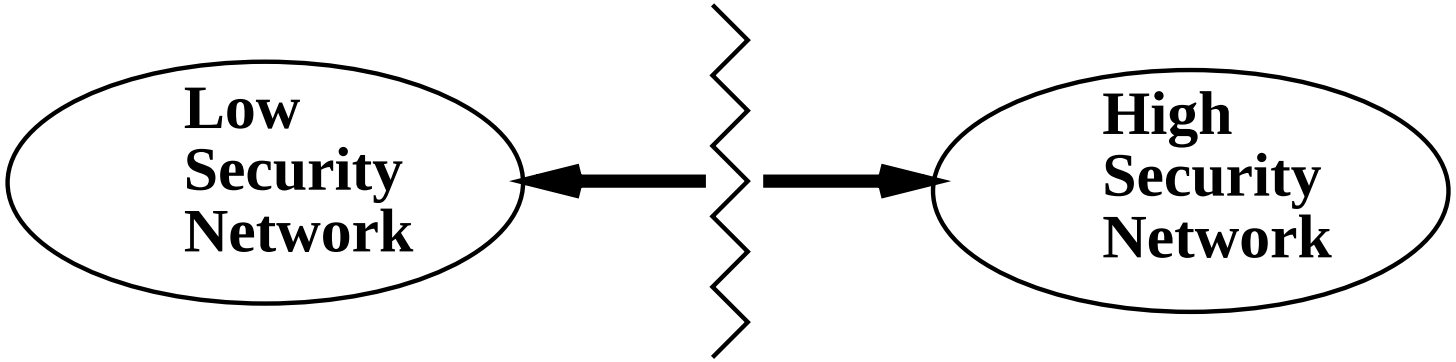
Introduction

- Enforcing Bell-LaPadula security policy
- Two networks: "High" and "Low"
- Data flows only from Low to High
- Problem: How?



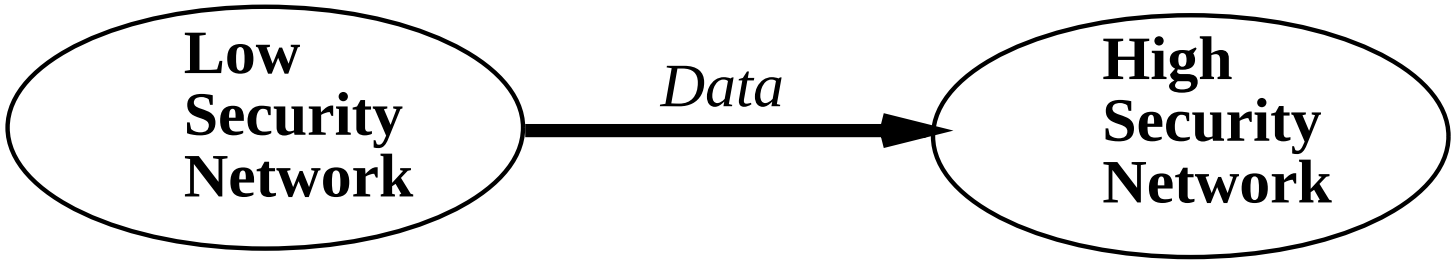
Simple Solutions: Isolation Method

- Physically isolate the two networks
- Since no data is exchanged, there is no unauthorized data exchanged either
- We would like some data flow



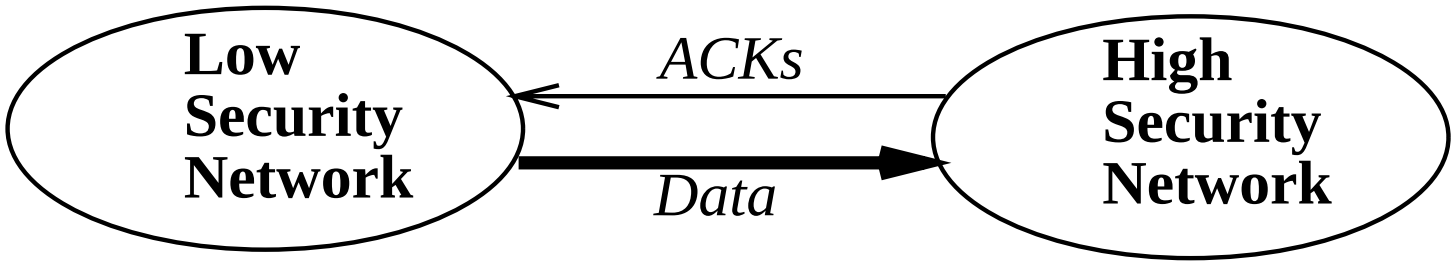
Simple Solutions: Blind Write-Up

- Connect the networks with a one-way fiber link
- No data flows from High to Low
- Problem: no reliability



Simple Solutions: ACK Filter

- Only ACKs flow from High to Low
- Problem: covert channels



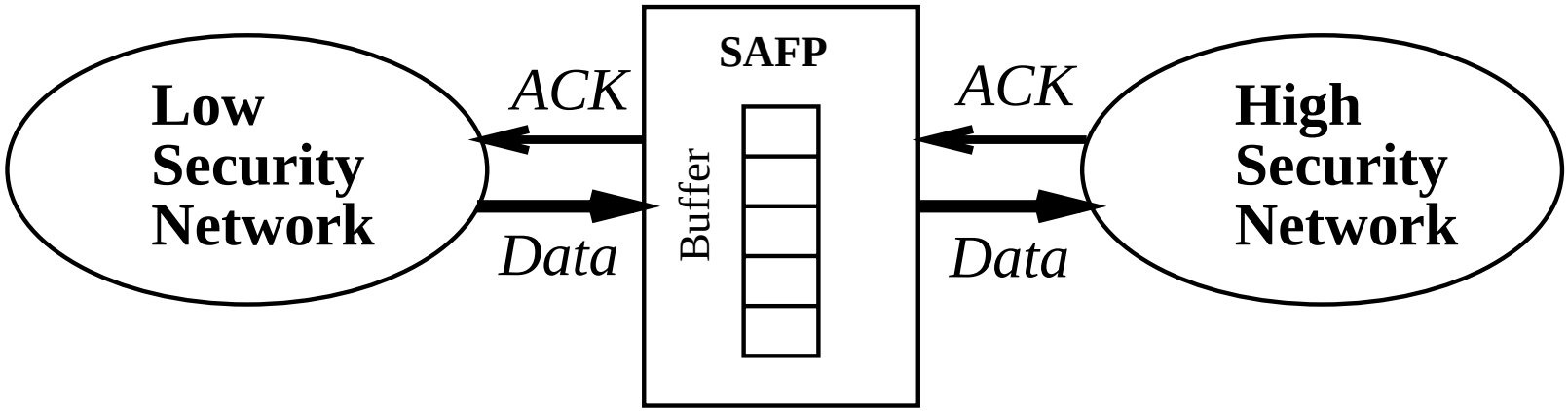
Previously Proposed Protocols

Providing TCP in one-way communication systems:

- **Store and Forward Protocol (SAFP)**
- **The Pump**
- **Upwards Channel**

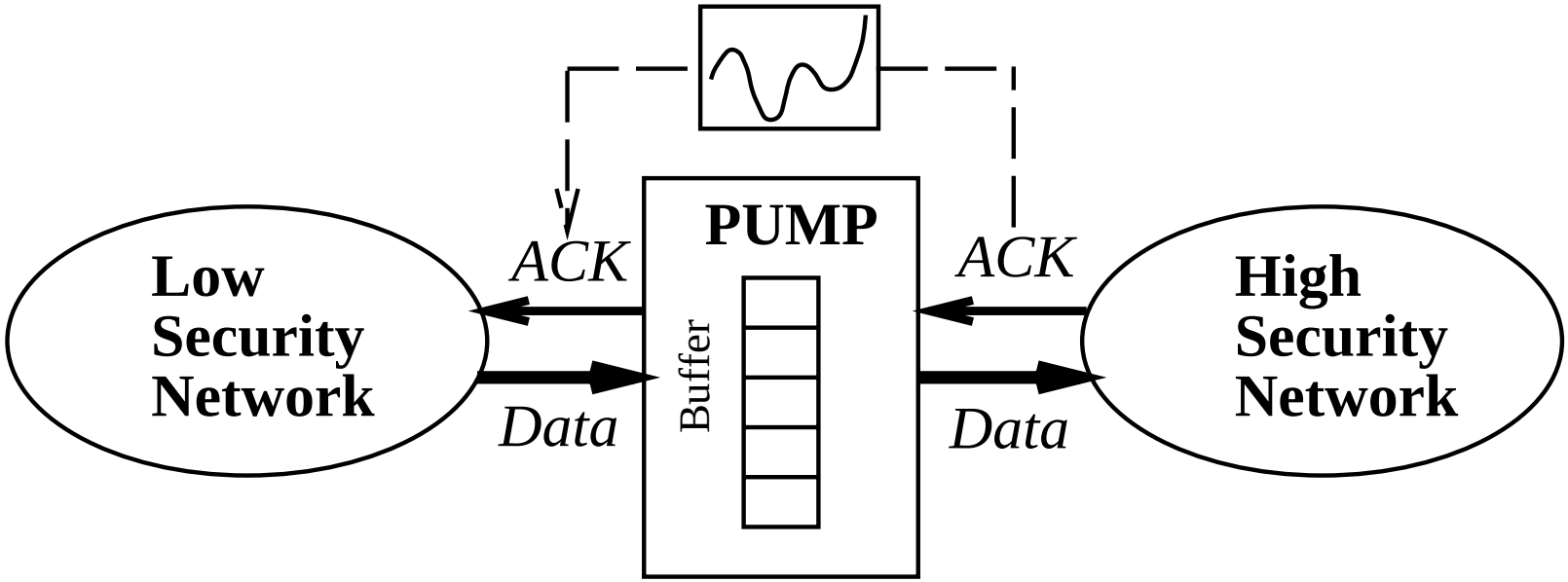
Store and Forward Protocol (SAFP)

- ACK Filter + Buffer
- Problem: large covert channel



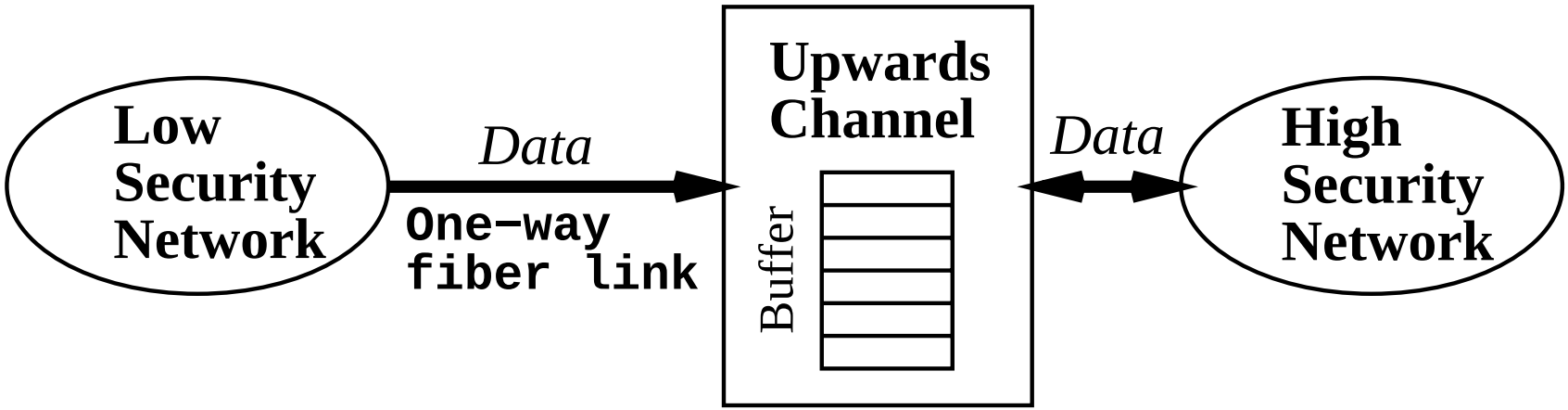
The Pump

- **SAFP + Historic Moving Average**
- **Problem: very hard to analyze**



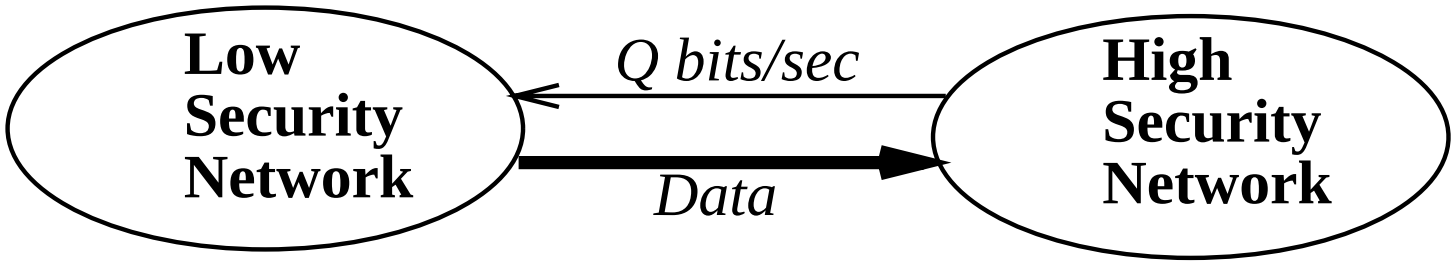
Upwards Channel

- Blind Write-Up + Buffer
- Problem: either unreliable or restriced to precise data rates

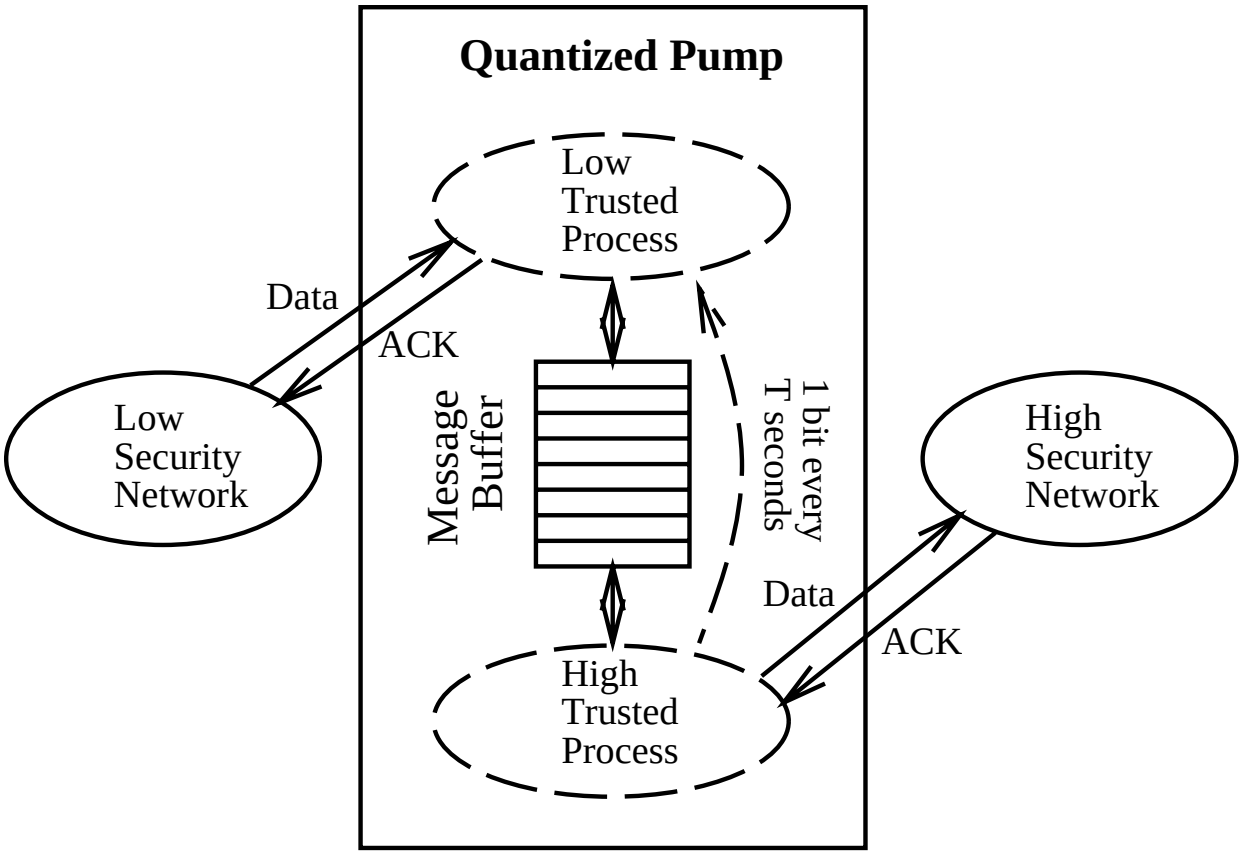


Quantized Pump Overview

- **Want to control covert channel bandwidth** *precisely*
- **Provable and easily analyzable**
- **Idea: use exactly as many bits as allowed**
- **How do we use those bits?**



Quantized Pump Implementation



- **One bit every T seconds between HTP and LTP**
- **Unbounded buffer size**

Quantized Pump

- **Covert channel bandwidth:** $Q = 1/T$ **bits/second**
- **Meaning of the bit passed every** T **seconds?**
- **Raise or lower the data rate by** R **bytes/second**
- **Maximum buffer size:**

$$\frac{1}{2}(L_{max}/R + 1)L_{max}T = O(L_{max}^2)$$

- **Throughput: 100% of SAFP's**

Logarithmic Quantized Pump

- **Different meaning of the bit passed between HTP and LTP**
- **Raise the data rate by R**
- **Lower the rate by twice the previous amount**
- **Maximum buffer size:**

$$T((\log L_{max} - \log R)(L_{max} + R) - L_{max} + 2R) =$$

$$O(L_{max} \log L_{max})$$

- **Throughput: 90% of SAFP's**

Linear Quantized Pump

- **Different meaning of the bit passed between HTP and LTP**
- **Raise the data rate by R**
- **Lower the data rate to zero**
- **Maximum buffer size:**

$$TL_{max} = O(L_{max})$$

- **Throughput: 45% of SAFP's**

Further Improvements

- Introduce random noise into communication bits
- Adaptive gateway: incorporate all three versions of Quantized Pump
- Only low trusted process involved
- Cannot be an exact algorithm

Summary

- Previously proposed protocols
- Introduced a new protocol: Quantized Pump
- Easy to configure and easy to analyze
- Has a provable bound on the covert channel bandwidth
- Comparable performance results