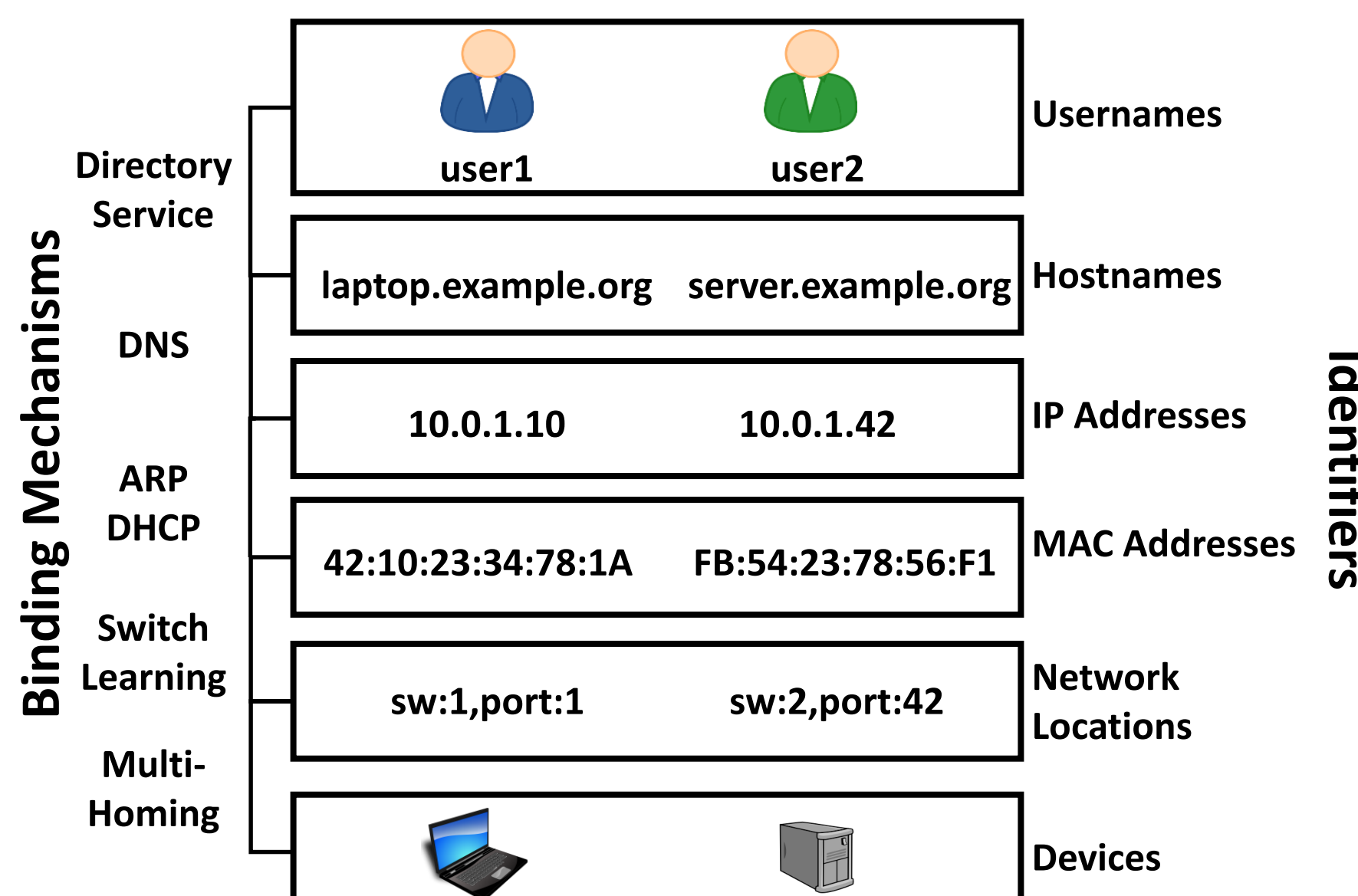


Identifier Binding Attacks and Defenses in Software-Defined Networks

Samuel Jero, William Koch, Richard Skowrya, Hamed Okhravi, Cristina Nita-Rotaru, and David Bigelow
 Purdue University, Boston University, MIT Lincoln Laboratory, and Northeastern University
 Appeared in *USENIX Security 2017*

Network Identifiers and Their Bindings

- Network Identifier: An Identifier for a device used at some layer of the network stack
- Used for forwarding, access control, and authorization
- Bound from higher layers to lower layers to actually send traffic

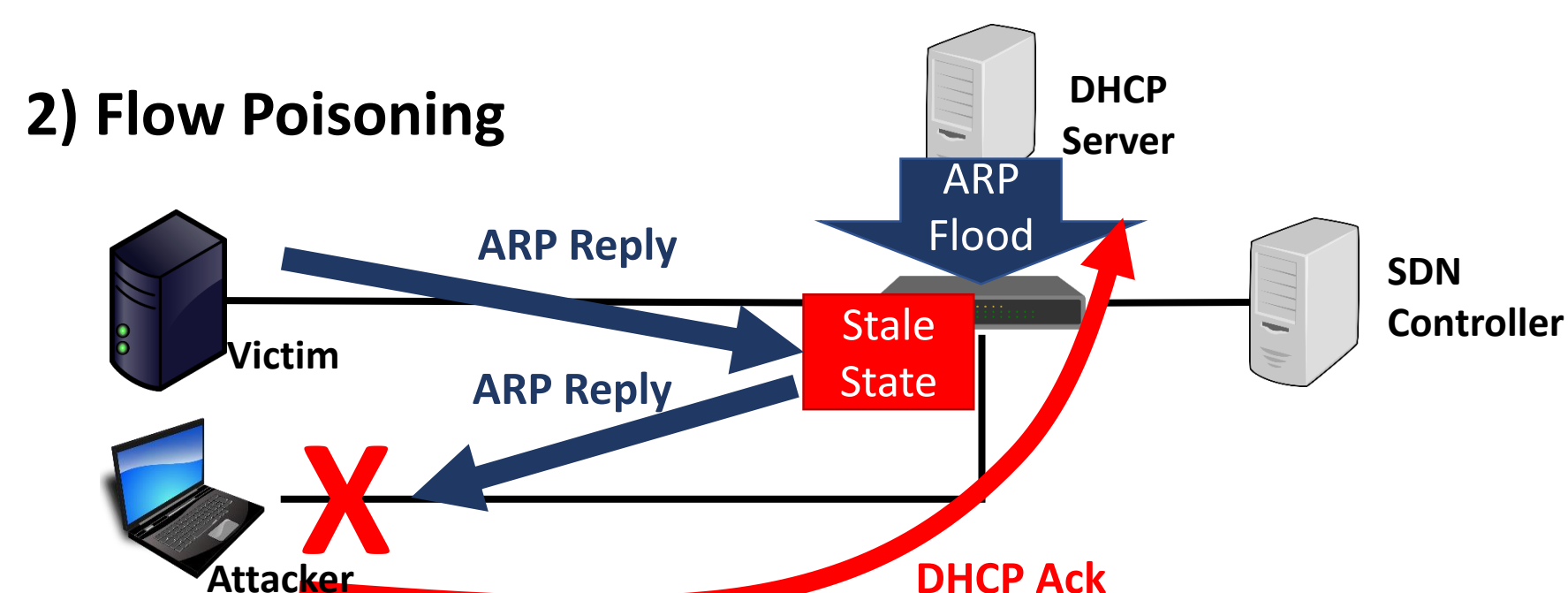
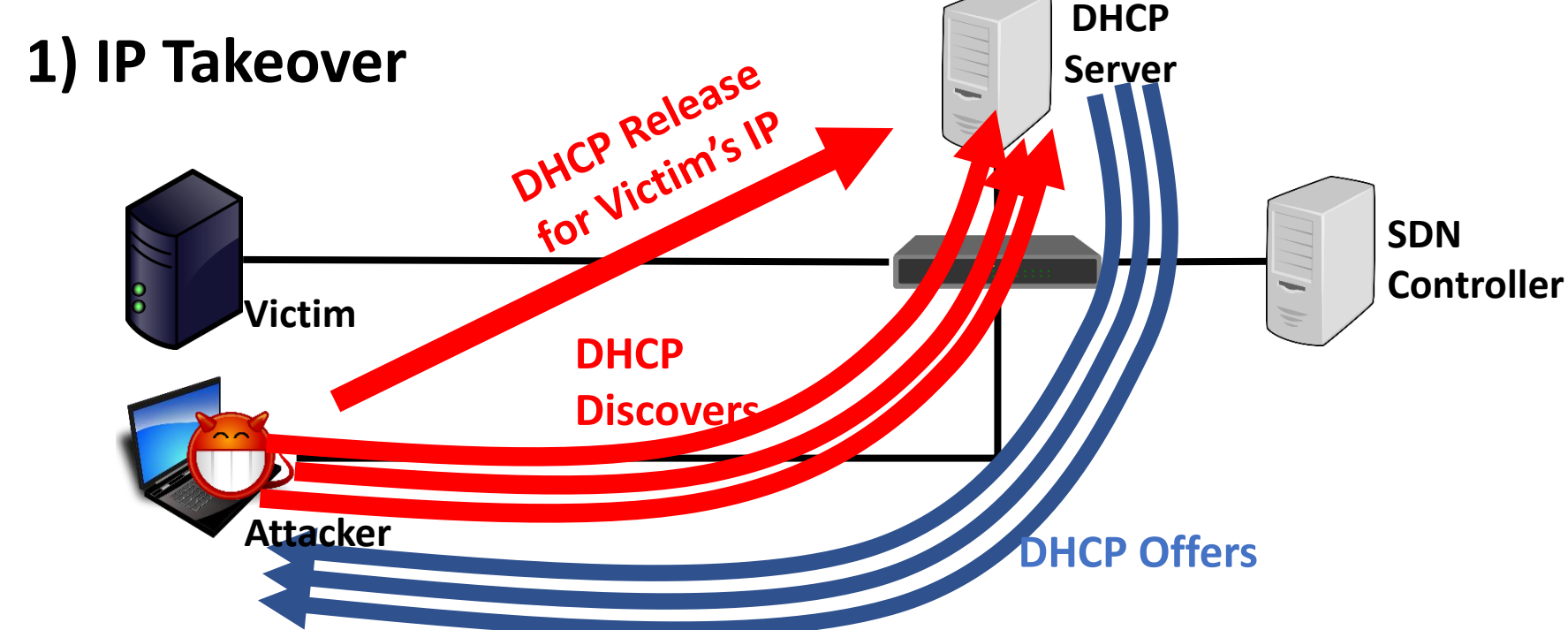


Bindings are done by insecure protocols

- No authentication
- Simple broadcast queries
- No cross-layer checks
- No additional checks on binding updates
- Mutable Identifiers

Persona Hijacking Attack

- Novel and extremely powerful identifier binding attack
- Achieves takeover of the victim's IP address and DNS name
- Persists for hours or days
- Attacker becomes the *owner-of-record* for the victim's IP address



Vulnerable Controllers

Controller	Experimentally Vulnerable	Probably Vulnerable*	Not Vulnerable
ONOS	X		
Ryu	X		
POX		X	
Floodlight		X	

* Based on Source Code Analysis

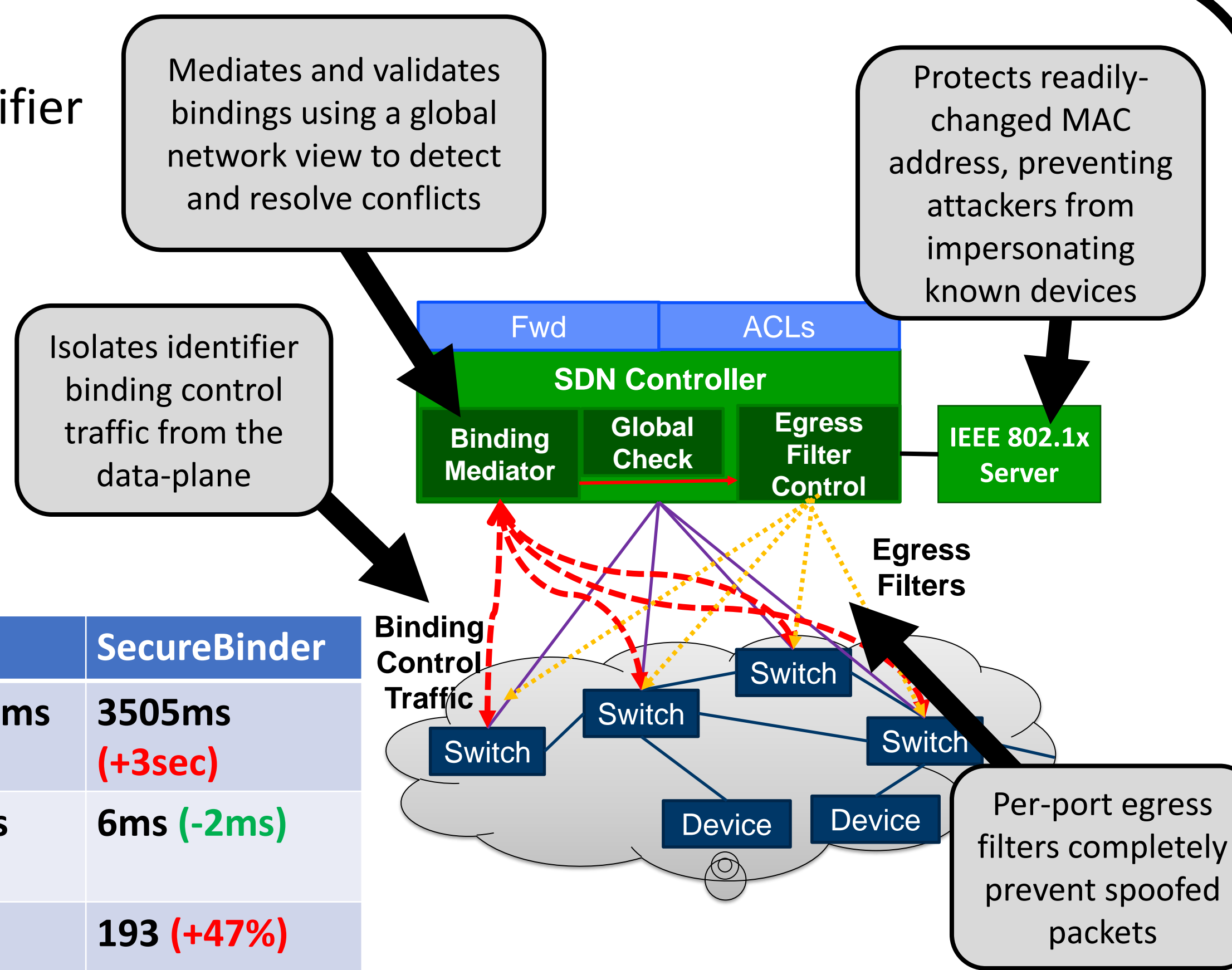
SecureBinder

- SDN-based defense to completely prevent identifier binding attacks
- Mediates identifier bindings
- Provides a root-of-trust for network identifiers

Evaluation

Attack	ONOS	SecureBinder
Persona Hijacking	X	✓
Host Location Hijacking	X	✓
ARP Spoofing	X	✓

Performance	ONOS	SecureBinder
Host Join Latency	505ms	3505ms (+3sec)
New Flow Latency	8ms	6ms (-2ms)
Pkt_ins (Load)	131	193 (+47%)



Acknowledgements and Contact Info

For more information about this project, contact: Samuel Jero <sjero@sjero.net>. Or see our paper in *USENIX Security 2017*.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. This material is based upon work supported by the Department of Defense under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense. © 2017 Massachusetts Institute of Technology. Delivered to the U.S. Government with Unlimited Rights, as defined in DFARS Part 252.227-7013 or 7014 (Feb 2014). Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed above. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work. This material is also based upon work partially supported by the National Science Foundation under Grant No. 1600266.