# SDNA : A Self-shielding Dynamic Network Architecture

## Problem

- With patience, a vulnerability in a computer network can be found and exploited
- Once inside, an attack can easily spread
- Prevent and limit attacks before detection
- 0-day, USB/email, compromised OS, etc.

Photo by Ethan Prater, used under Creative Commons Attribution 2.0 Generic (CC BY 2.0) License

## Goals

- Disrupt planning & effectiveness of attacks
- Prevent first node from being attacked
- Prevent spread after a successful attack
- Provide additional information to improve detection of and recovery from attacks

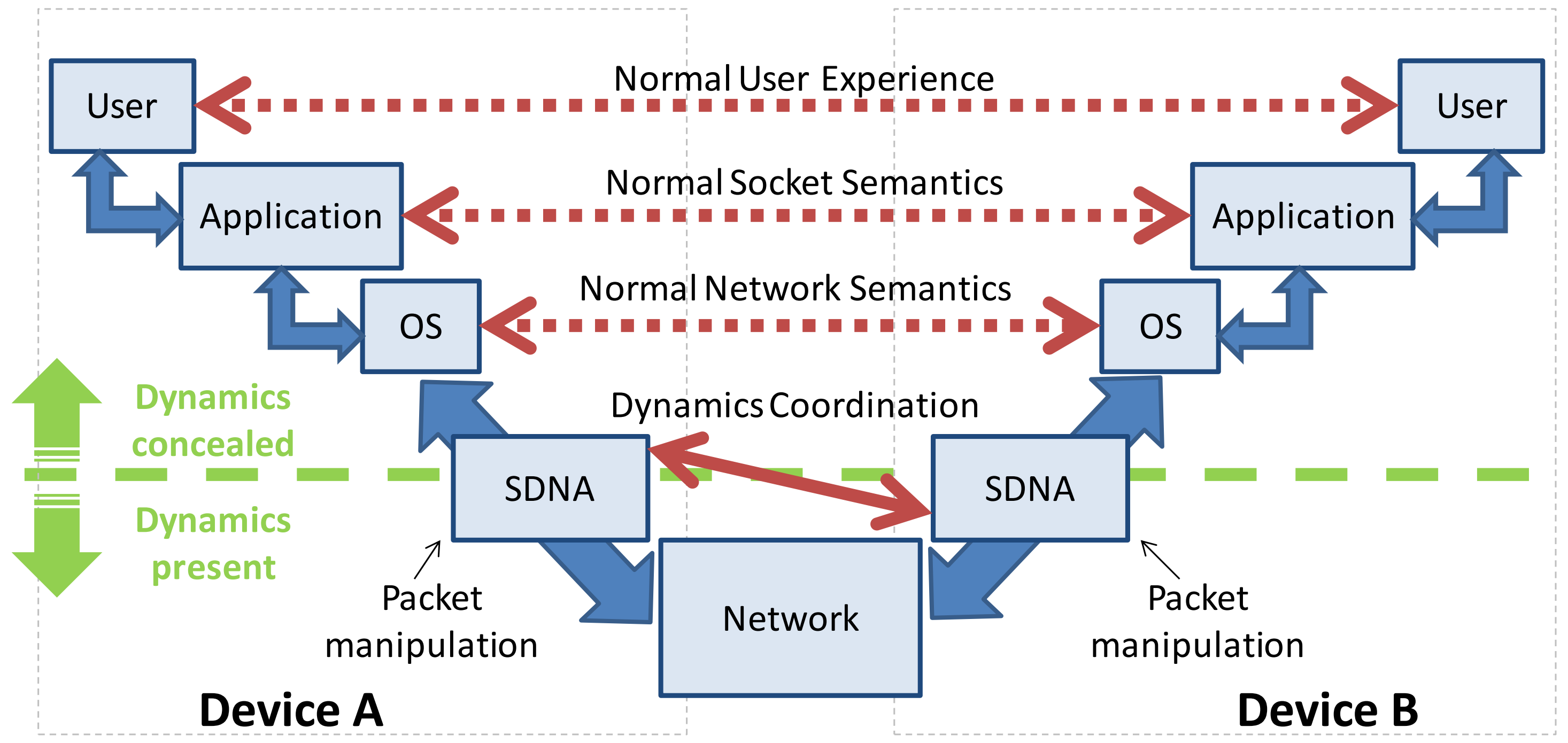
## Sponsor

Walt Tirenin, AFRL
FA8750-10-C-0089 and FA8750-11-C-0179

## Contact

Justin Yackoski : jyackoski@i-a-i.com 301-294-4251
http://www.i-a-i.com

## SDNA Key Concepts



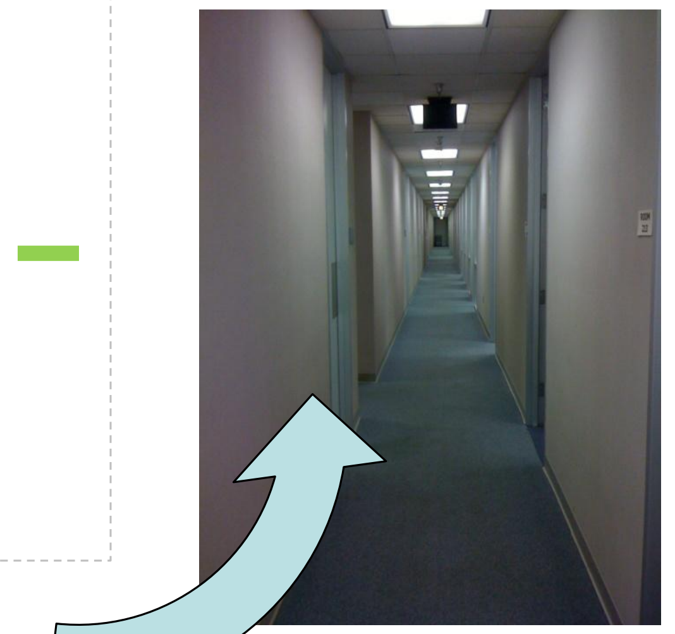


Photo by user ilovebutter, used under Creative Commons Attribution 2.0 Generic (CC BY 2.0) License

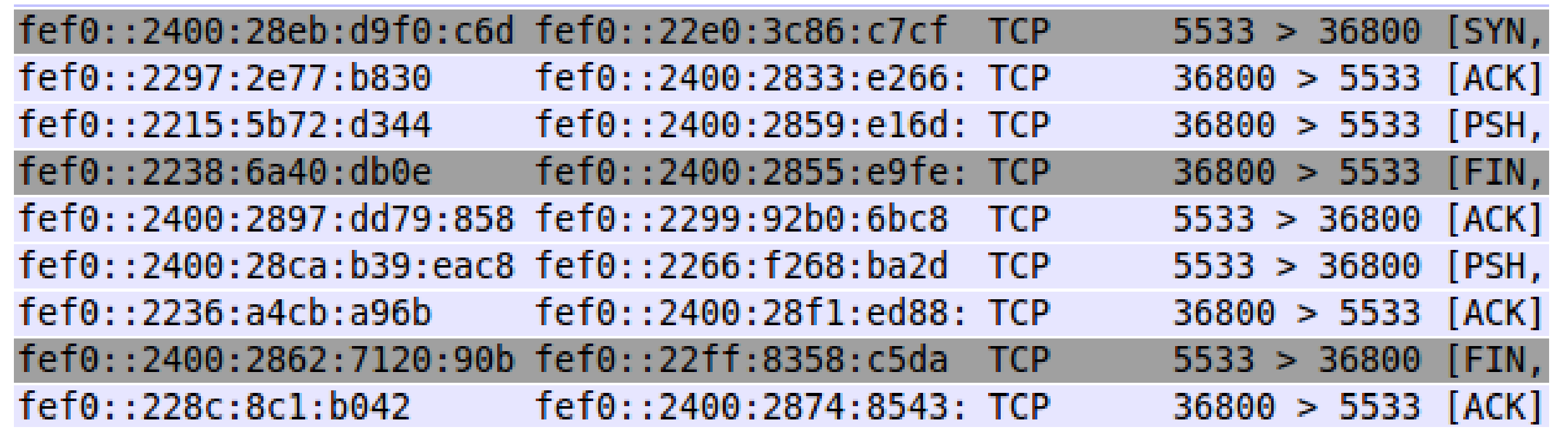
**Like a hallway with many doors…**

Burden on attacker, all choices except 1 are a trap
Must make choice to test its correctness
Correct door constantly changes, cannot follow
Not just "security through obscurity"

- Integrated, decentralized architecture
- IPv6 based, IPv4 compatible
- Continually change network's appearance in multiple ways
- Network access is managed & protected by a hypervisor
- Transparent to OS, apps, and user
- Cryptographically strong
- Network is secure by default

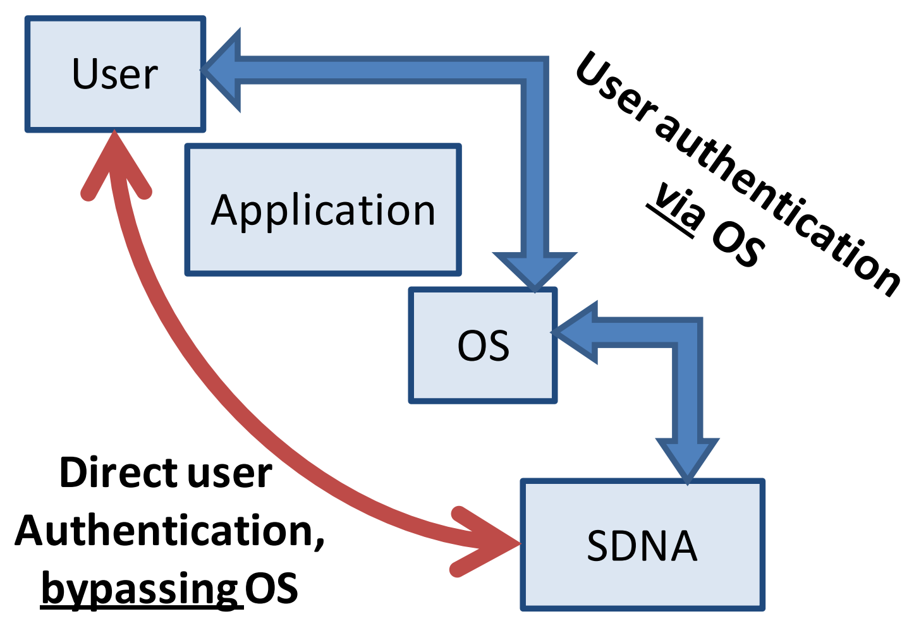
## Security

- Addresses cannot be meaningfully observed or used to locate/identify important nodes
- Network appearance differs per user & node
- Sender of a packet can be verified
- Secure against a compromised OS
- Non-SDNA devices/packets are easily detected and dropped/honeypotted



```
fef0::2400:28eb:d9f0:c6d fef0::22e0:3c86:c7cf  TCP      5533 > 36800 [SYN,
fef0::2297:2e77:b830     fef0::2400:2833:e266: TCP      36800 > 5533 [ACK]
fef0::2215:5b72:d344     fef0::2400:2859:e16d: TCP      36800 > 5533 [PSH,
fef0::2238:6a40:db0e     fef0::2400:2855:e9fe: TCP      36800 > 5533 [FIN,
fef0::2400:2897:dd79:858 fef0::2299:92b0:6bc8  TCP      5533 > 36800 [ACK]
fef0::2400:28ca:b39:eac8 fef0::2266:f268:ba2d  TCP      5533 > 36800 [PSH,
fef0::2236:a4cb:a96b     fef0::2400:28f1:ed88: TCP      36800 > 5533 [ACK]
fef0::2400:2862:7120:90b fef0::22ff:8358:c5da  TCP      5533 > 36800 [FIN,
fef0::228c:8c1:b042      fef0::2400:2874:8543: TCP      36800 > 5533 [ACK]
```

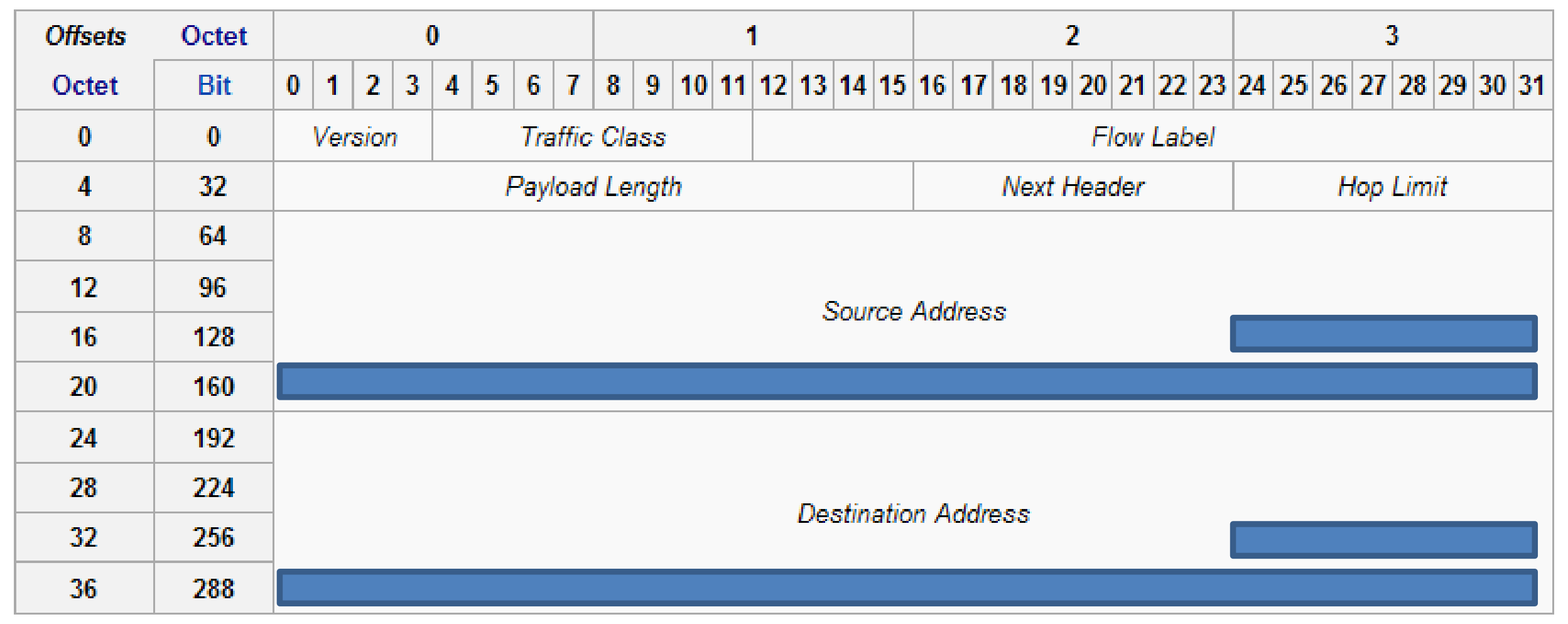
Example capture of packets in an SDNA network


User
Application
OS
SDNA
User authentication via OS
Direct user Authentication, bypassing OS

## Feasibility/Usability

- No changes to OS or apps
- Use existing CAC systems
- No changes to network hardware
- Dynamics are hidden from legitimate users

Use large IPv6 address space to create dynamics



| Offsets | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 0 | 0 | Version | | | | Traffic Class | | | | | | | | Flow Label | | | | | | | | | | | | | | | | | | | |
| 4 | 32 | Payload Length | | | | | | | | | | | | | | | | Next Header | | | | | | | | Hop Limit | | | | | | | |
| 8 | 64 | Source Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | 96 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 16 | 128 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20 | 160 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 24 | 192 | Destination Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 28 | 224 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 32 | 256 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 36 | 288 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Source: http://en.wikipedia.org/wiki/IPv6_packet

Approved for Public Release; Distribution Unlimited: 88ABW-2012-2986,23-May-2012