SDN Security

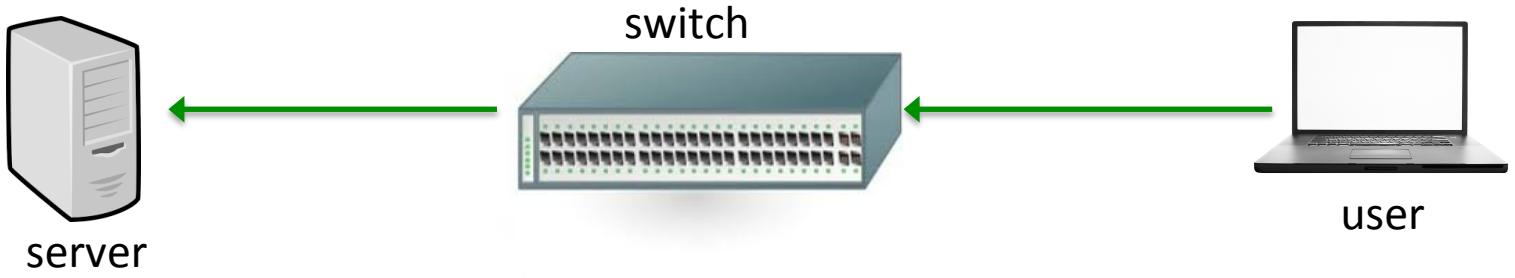
Matt Bishop, Brian Perry
University of California at Davis

Network Switches

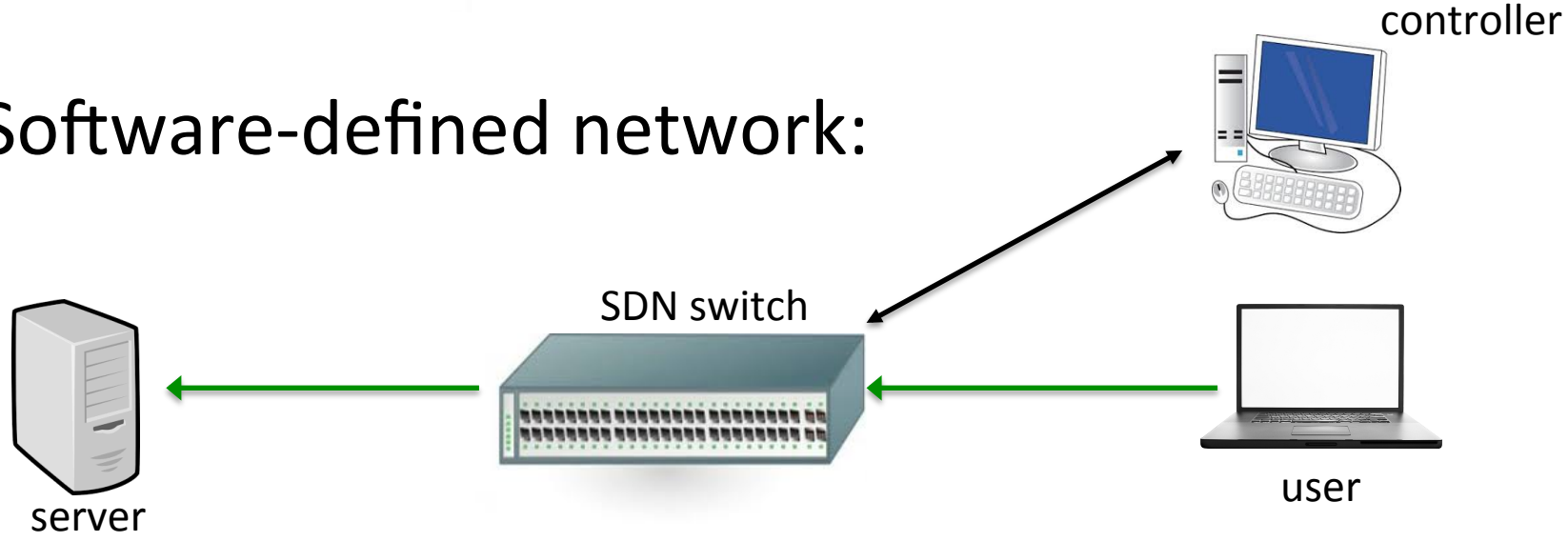
- Conventional switch: closed system
  - Support manufacturer-specific control interfaces
  - Control, data planes embedded in them
  - Changes in protocols, services, etc. usually require replacing or updating switch
- SDN: decouple control, data planes
  - Control plane controlled by a centralized controller on a computer (PC, for example)
  - Can program switch via controller
  - Easy to propagate changes in protocols, services, etc.

What Does This Mean?

- Traditional set-up:



- Software-defined network:



Security

- Trust, maintenance, resilient design, etc. common to both
- Authentication, authorization in SDN network more complicated
  - As commands and changes come on the fly, need to be sure these come from an authorized source
  - Can have dynamic policy for handling flows
  - “Apps” can perform additional security functions

Security Using the Switch

- Switch provides, assists security mechanisms
  - OpenFlow Random Host Mutation
  - Provide data for anomaly-based intrusion detection (more accurate than ISP-driven IDS)
  - Enforce dynamic access control policies based on flow-level information
  - Various security applications
    - Edge-based authentication gateways
    - Security application development frameworks

Security *of* the Switch

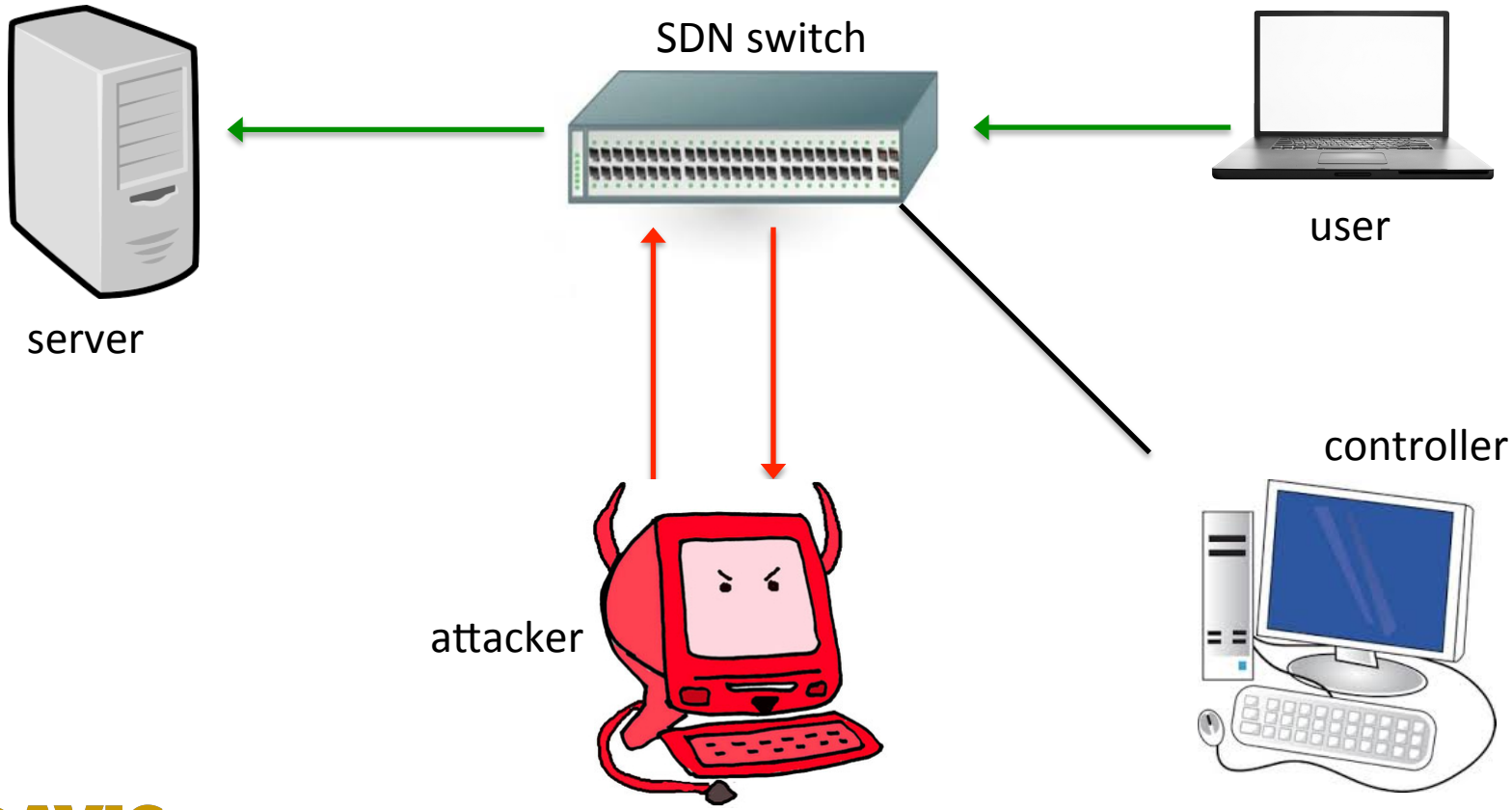
- Software
  - Verify
    - Various groups doing this with OpenFlow; not so much with others
    - Check for misconfigurations within a single flow table
  - Implement a security enforcement kernel
  - Lots of control/data plane interactions can disrupt operations
- Link to controller(?)
  - Ensure connection to controller is secured (TLS)
  - Disable passive listening (require authentication)

Our Approach

- Controller is a ordinary computer — with all the vulnerabilities of an ordinary computer
  - So, attack that
  - Once in control of the controller, have fun!
- Also applies if we can impersonate the controller
  - Here's where the listener port comes into play
- This also considers misconfigurations downloaded from the controller
  - Must assume humans are fallible

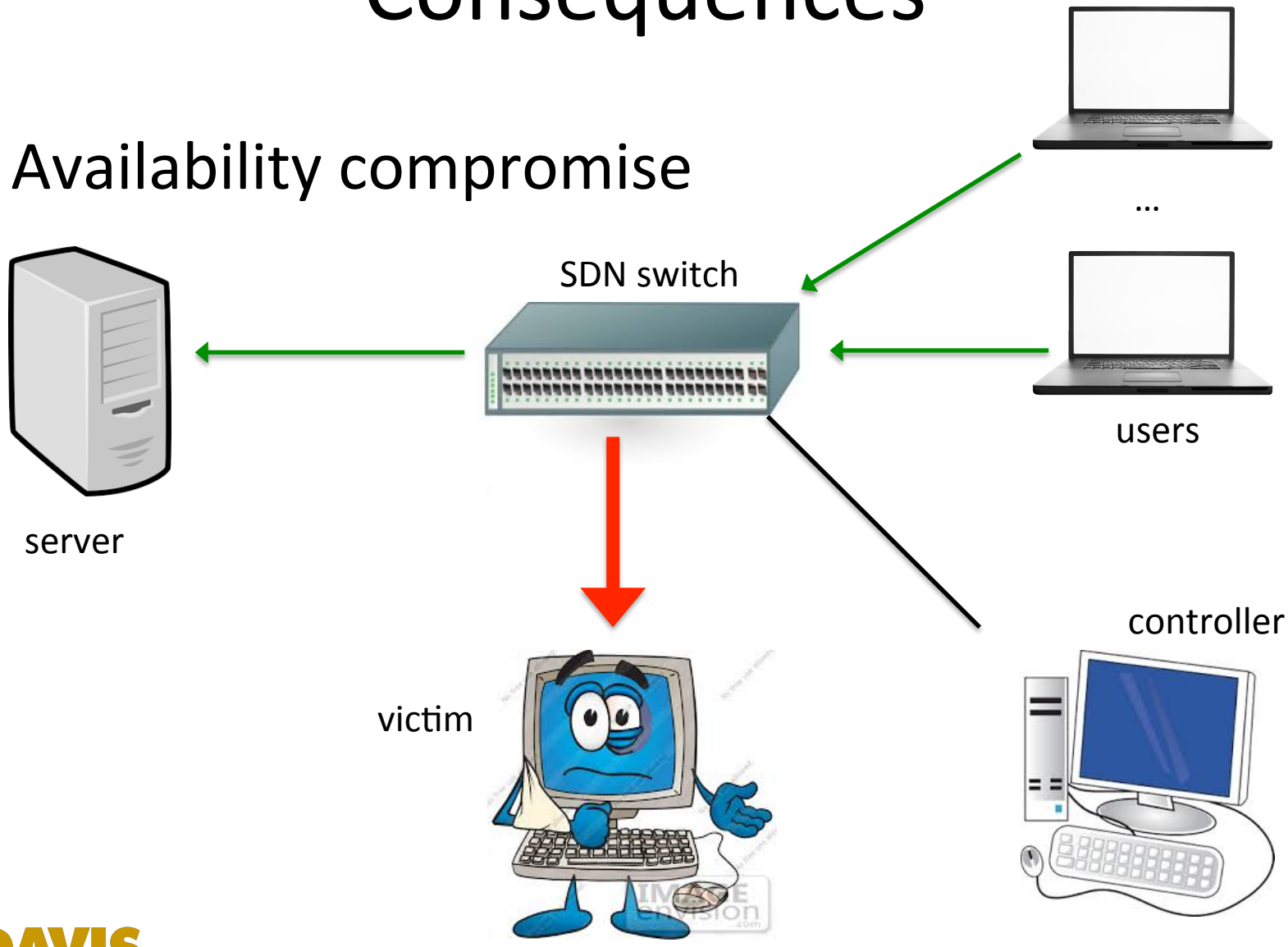
Consequences

- Confidentiality, integrity compromise



Consequences

- Availability compromise



Key Points

- You can gain security with SDN, but you can also lose security (and *vice versa*)
- Security problems with SDN can wreak havoc on networks that depend on them
  - Like GENI
- Introducing powerful technology also introduces the risk of that power being used against you
  - And the threats may not come from where you expect!

Conclusion

- Security of the switch is important
- Security of whatever can *control* the switch even more so
  - Most computers vulnerable to attack
  - Best to use dedicated, stripped-down system as controller
  - If you can isolate it, so much the better

Thanks to …

- Abhishek Gupta
- Saadet Sedef Savas
- Steven Templeton

Funded by the GENI Projects Office through Contract #950012166, Prime Sponsor (NSF) Award CNS-1344668

About Me

Matt Bishop
Computer Security Laboratory
Department of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562 USA

phone: +1 (530) 752-8060
email: bishop@ucdavis.edu
web: http://seclab.cs.ucdavis.edu/~bishop