Sysadmins and the law

If you think your job sucks, imagine Federal Prison.

Disclaimer

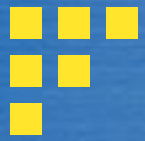
- This talk discusses current U.S. Federal law. Each US state has its own laws that may differ from Federal law.
- This is not legal advice. If you have legal questions or issues, consult with a licensed attorney in your jurisdiction.
- This area of law is in flux. What's legal today may change next month.

Acknowledgements

This research would not have been completed without help from:

Temple University Beasley School of Law

The Circuit Executive's Office of the U.S. Court of Appeals for the Third Circuit



Overview

- What content may a sysadmin look at on their network, and when?
- What is protected traffic, and what is not?
- How can you protect yourself and your organization from legal troubles?

Competing Statutes

- 4th amendment, U.S. Constitution
- Wiretap / Electronic Communications Privacy Act (18 U.S.C §§ 2510-2522)
- Stored Communications Act (18 U.S.C. §§ 2701-2711)
- Pen Register/ Trap and Trace (18 U.S.C. § 3121)
- State and Local statutes

4th Amendment

- "The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable** searches and seizures, shall not be violated…"
- Does not apply to non-government actors
- However, some states allow civil suits for 'intrusion into seclusion' by private actors

Wiretap/ECPA Title 1

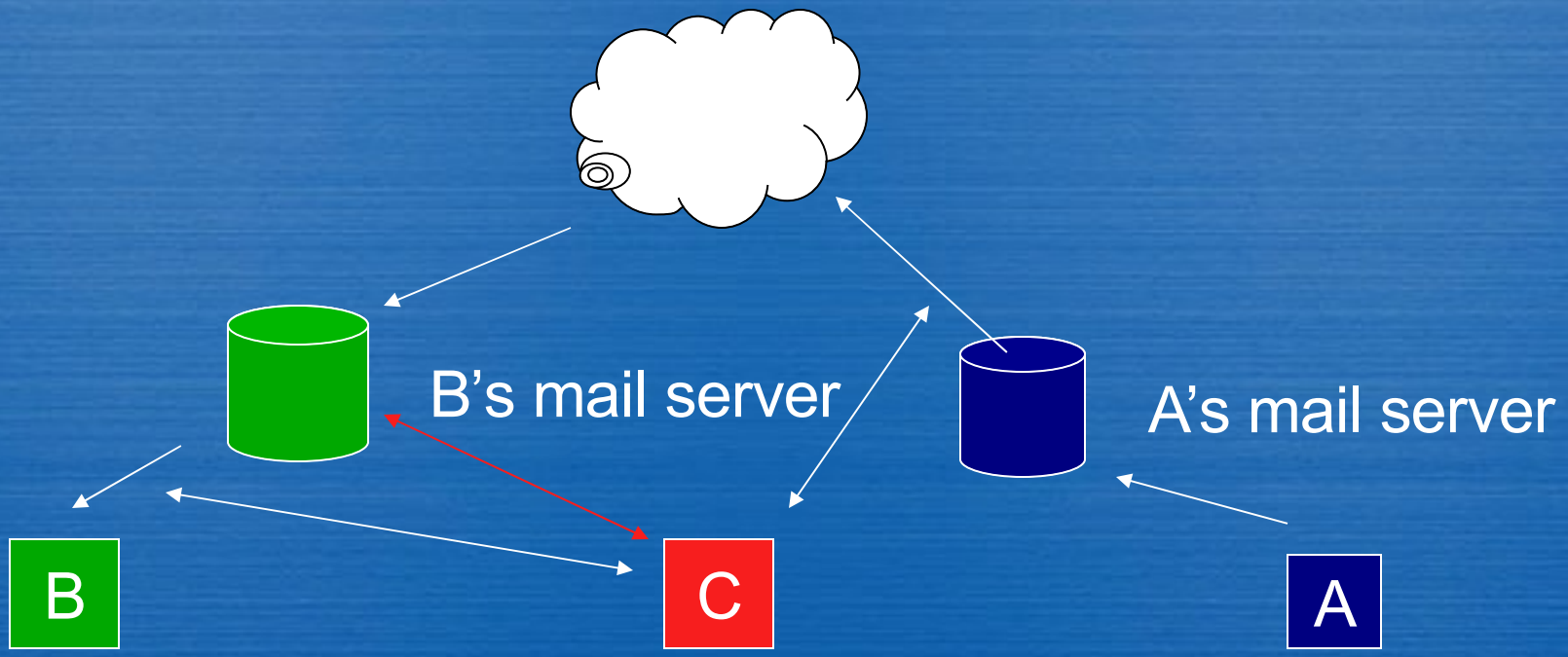
- Wiretap law originally enacted in Omnibus Crime Control act of 1968
- Significantly updated in 1986 by ECPA
- Updated again in 2001 by PATRIOT act

Wiretap Act

- "Interception" : acquisition of the **contents** of any …, electronic, or oral communication through the use of any … device. 18 USC § 2510
- Interception only when contemporaneous with transmission- not from storage (Steve Jackson Games v Secret Service)
- Federal prison up to five years, and victims may sue for damages and legal fees

What does interception look like?

A is sending email to B
C wants to read the email before B does



Interception exceptions

- Recipient (intended recipient of communication)
- Service provider agents and employees, to provide service,to protect the rights or facilities of the service provider,to comply with a court order or wiretap order or with the permission of the user
- To determine the source of harmful electronic interference
- To lawfully investigate a computer trespasser with the owner's consent, provided that no innocent communications are intercepted

Stored Communications Act

- Accessing a ‘stored communications service’ without permission or exceeding granted permissions and obtains, alters or prevents authorized access to information stored within
- If done for profit, up to five years first offense, ten years for subsequent offenses, and/or fine. Otherwise one/five years or fine
- Exceptions:
  - Owner of service
  - For user to access a message from or intended for them

Pen Register/Trap and Trace

- Pen Register- device to list of all phone numbers, time and duration dialed from one phone
- Trap and Trace-device to list all phones that have dialed one phone number, when and for how long
- Neither may acquire the **contents** of communications

Pen Register/Trap and Trace restrictions

- Providers may use either
  - With informed consent of customer
  - For billing purposes
  - For testing/maintenance/operation of service
  - To protect service,users or connected networks from illegal or abusive acts
  - Under Court wiretap order

Pen Register/Trap and Trace, continued

- Not limited to voice/wire
- Could be used to describe sniffer limited to TCP/IP headers
- Could be used by provider without permission of user, if no innocent content is captured

Some important cases

Steve Jackson Games v Secret Service (1995)

- Reading email from disk is not interception - must be at same time.

Garrity v John Hancock (2002)

- Employees have no implied expectation of privacy in work email

Muick v Glenayre (2002) Non-government employees generally have no right in work PC contents unless privacy is stated or implied

Councilman v US (2005)

- Provider offers free email to customers and reads emails from competitors
- Changes rule - interception no longer needs to be contemporaneous with receipt- and not only email!
- Provider protection becomes narrower- interception must be for business purposes

What does all this mean?

- Providers may intercept some communications to protect themselves, connected networks and their users
- Stored communications have less protection from providers than communications being transmitted
- Councilman is good law only for 1st Circuit- but may eventually replace Steve Jackson in rest of country

How to protect yourself?

- Get the consent of your users to capture packets, in writing-either in the TOS or by a separate contract rider
- Get permission from your employer, in writing
- Have a sniffer policy- when, how and where and who may use them