

# FlashPatch: Spreading Software Updates over Flash Drives in Under-connected Regions

Henry Corrigan-Gibbs  
*Stanford*

Jay Chen  
*NYU Abu Dhabi*

5<sup>th</sup> ACM DEV – San Jose, California  
5 December 2014

Expensive, low-bandwidth  
connection...

...good enough for email





Download and install updates for your computer

14 important updates are available  
37 optional updates are available

14 important updates selected,  
378.3 MB - 1,197.3 MB

Install updates

The screenshot shows a Windows Update notification window. It features a yellow shield icon with an exclamation mark on the left. The main text reads "Download and install updates for your computer". Below this, it states "14 important updates are available" and "37 optional updates are available". On the right side, it says "14 important updates selected, 378.3 MB - 1,197.3 MB". At the bottom right, there is a button labeled "Install updates".

Wait a minute...  
**1,197.3 MB !?!?!?**

The text is contained within a white, cloud-like speech bubble with a black outline. The first line says "Wait a minute..." and the second line says "1,197.3 MB !?!?!?" in red, bold font.

Let's do the math

**Offline computers are *never* able to download updates.**

Example: 100

## Cost

- 100 MB download: **USD 5.64** (MTN Nigeria)
- Daily GDP per capita: USD 8.23 (World Bank)

## Time

- On EDGE, get 120 Kb/s max throughput
- **Two hours** to download

# Paradox of Updates

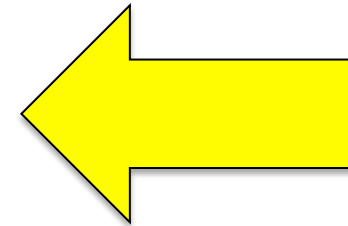
- If you DO update
  - Expensive
  - Time-consuming
  - Unclear benefits
- If you DO NOT update
  - Vulnerable to **flash-borne malware**
  - Software bugs

Is there a better way to spread  
software updates?

# Goal

Build a system for distributing software updates that is:

1. **Realistic**: no new hardware
2. **Easy to use**: no training
3. **Effective**: faster/cheaper than *status quo*



# Outline

- **Motivation**
- System design
- Evaluation
- Conclusions

# Outline

- Motivation
- **System design**
- Evaluation
- Conclusions

# The Idea

Use a vector for **virus transmission...**



...as a vector for **update propagation.**



# Flash Drives

...are ubiquitous



...are high-bandwidth



... circulate quickly

# FlashPatch

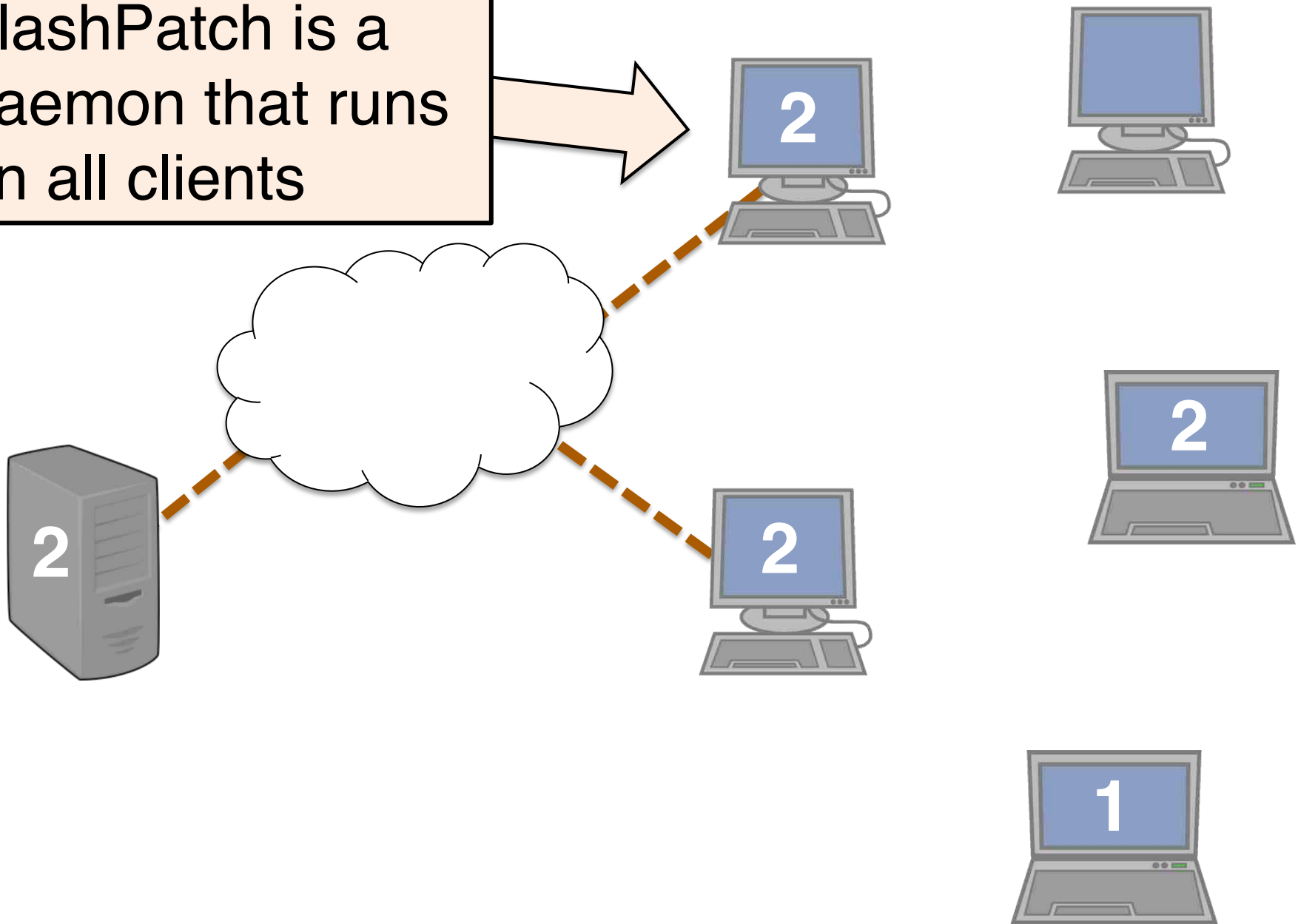
Copy updates to/from flash drives  
as they go by

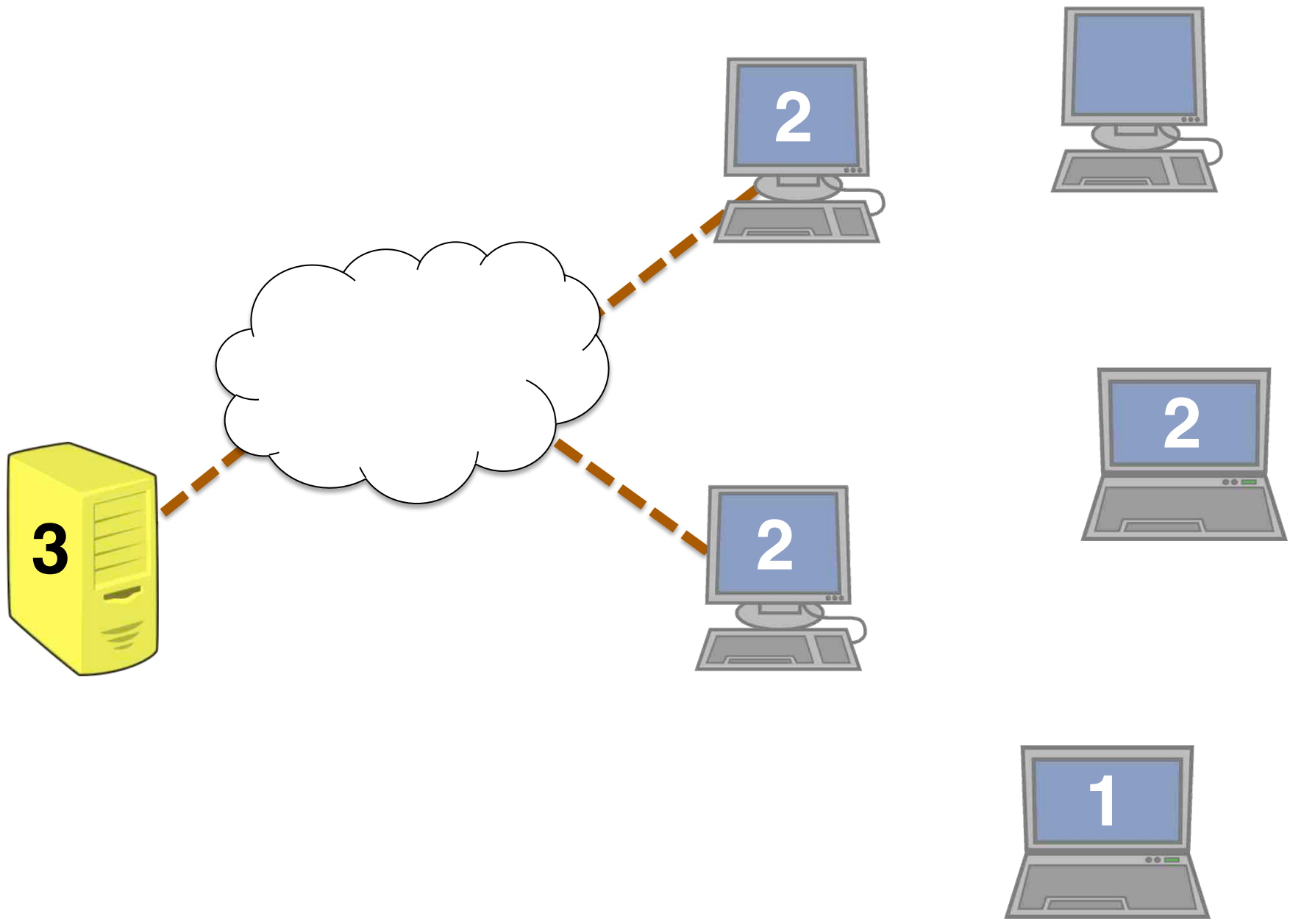
NO CHANGE in  
user behavior  
required!!!

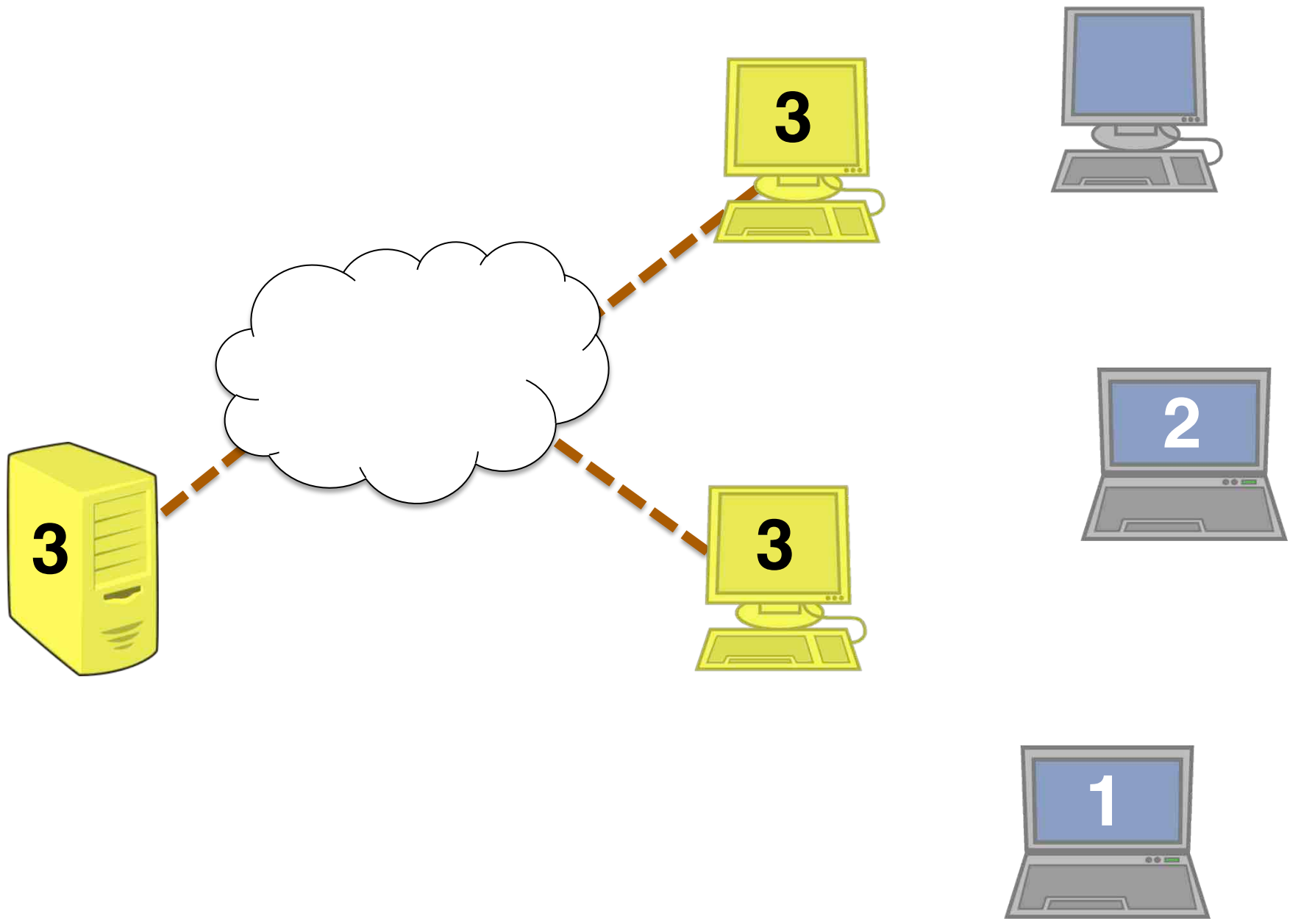


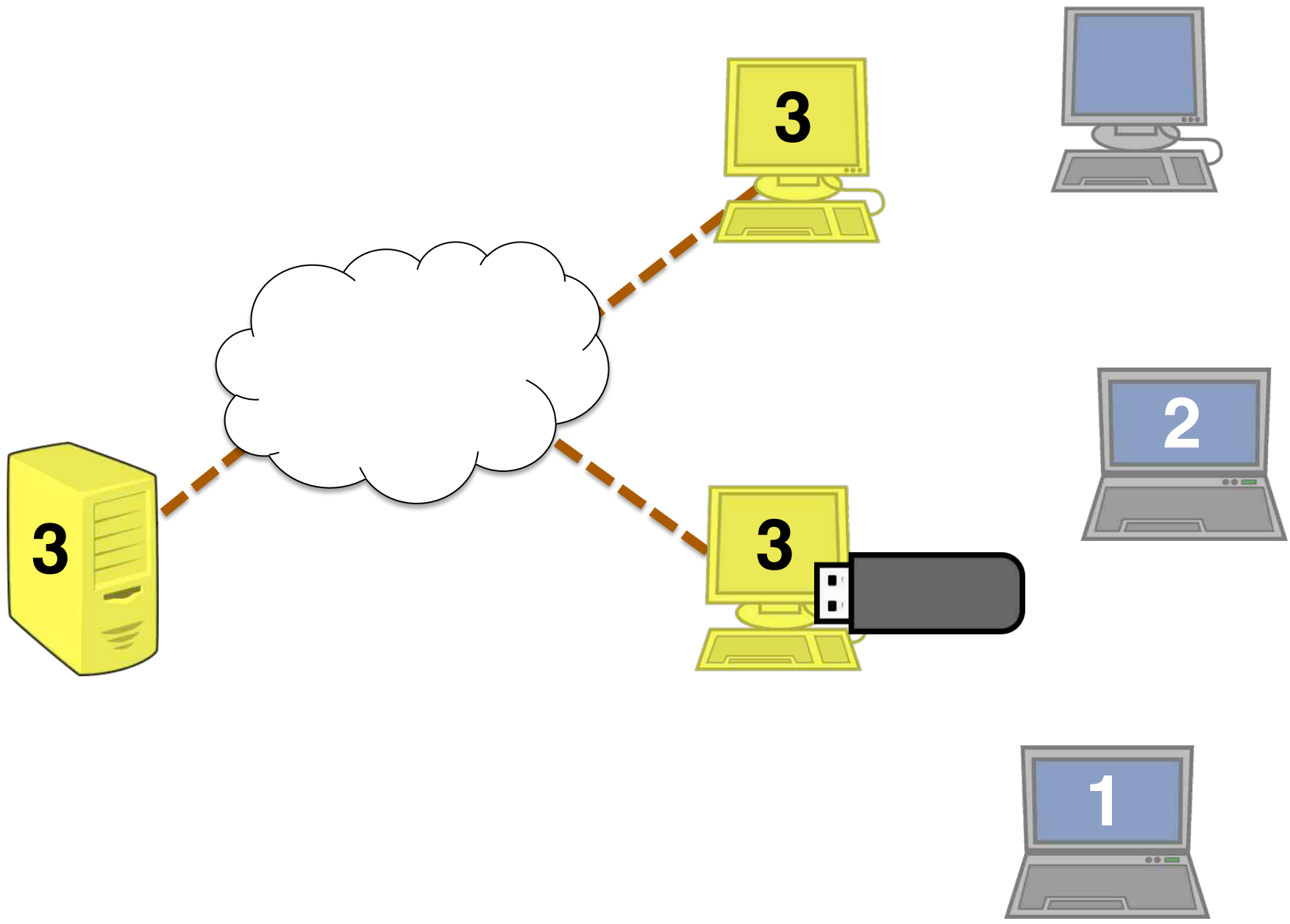
Updates “piggyback” on the  
**pre-existing flow** of flash drives

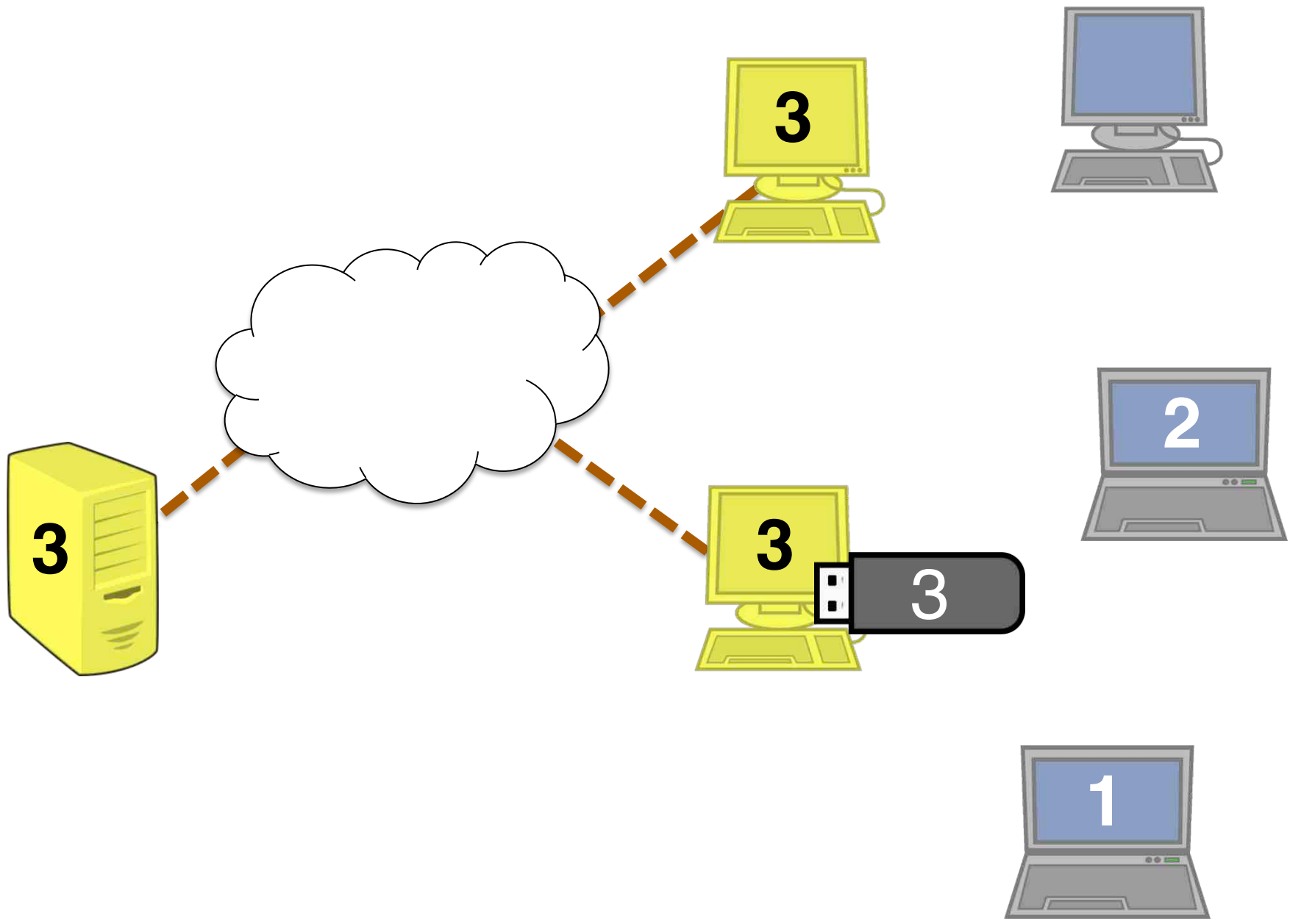
FlashPatch is a daemon that runs on all clients

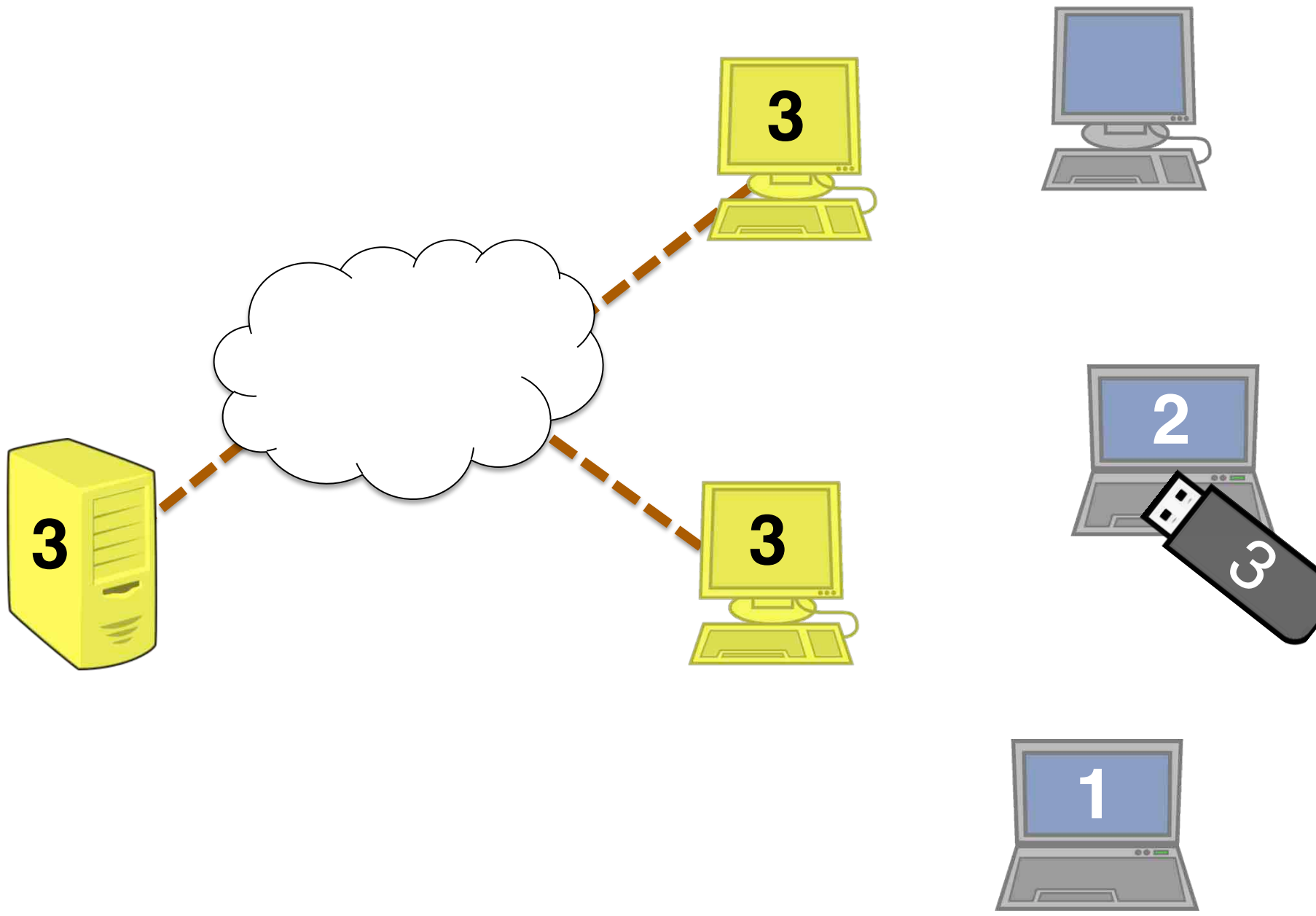


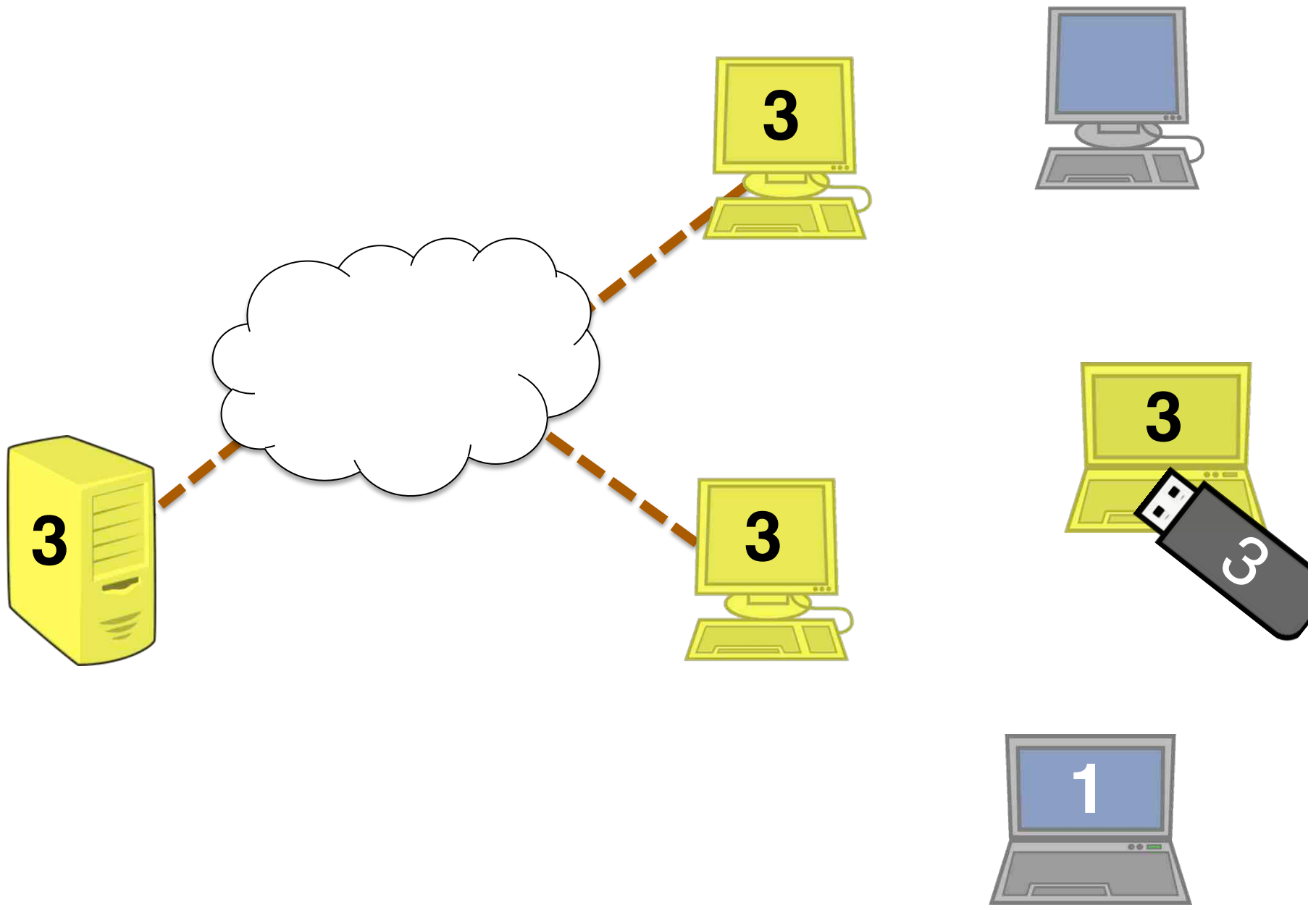


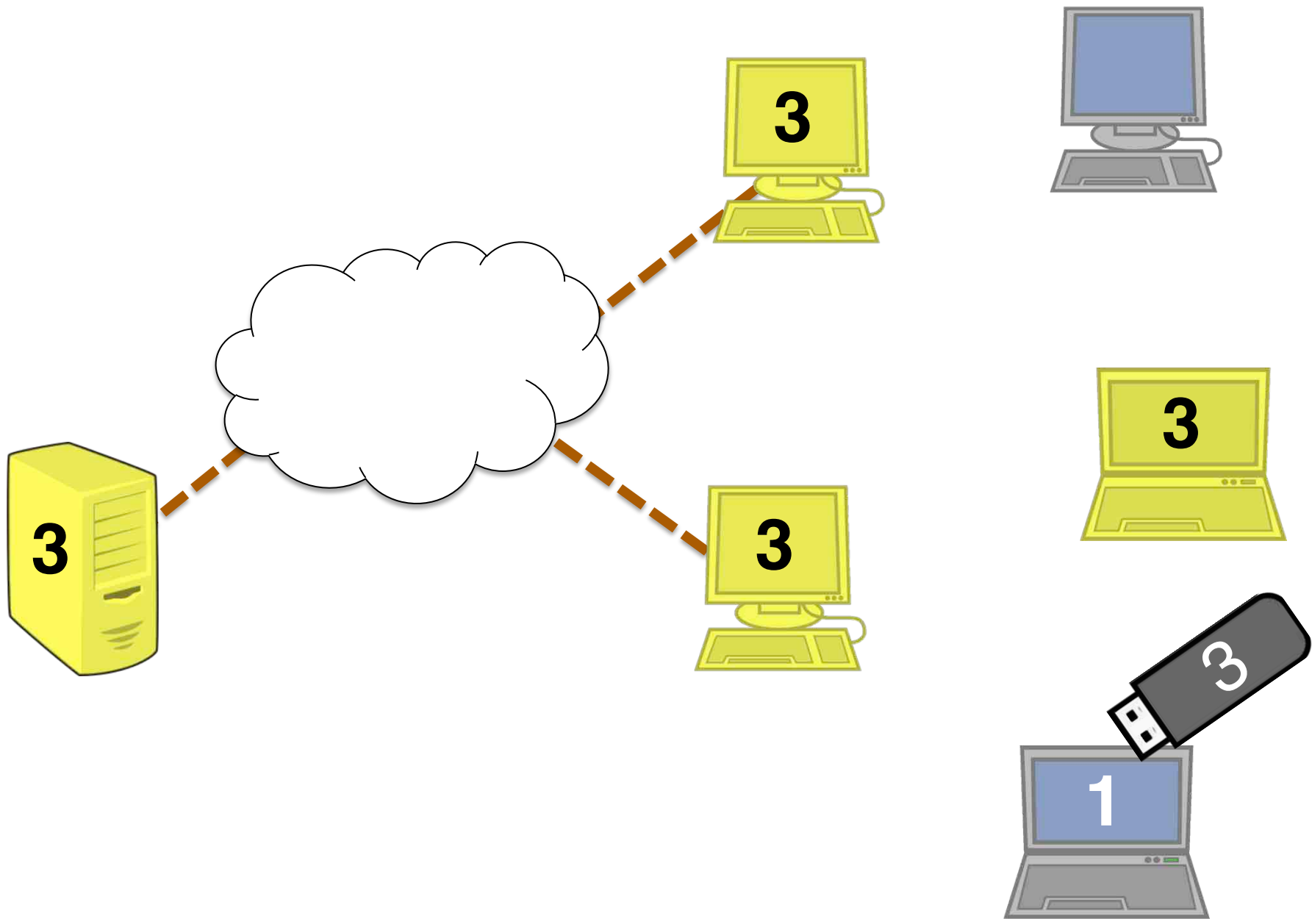


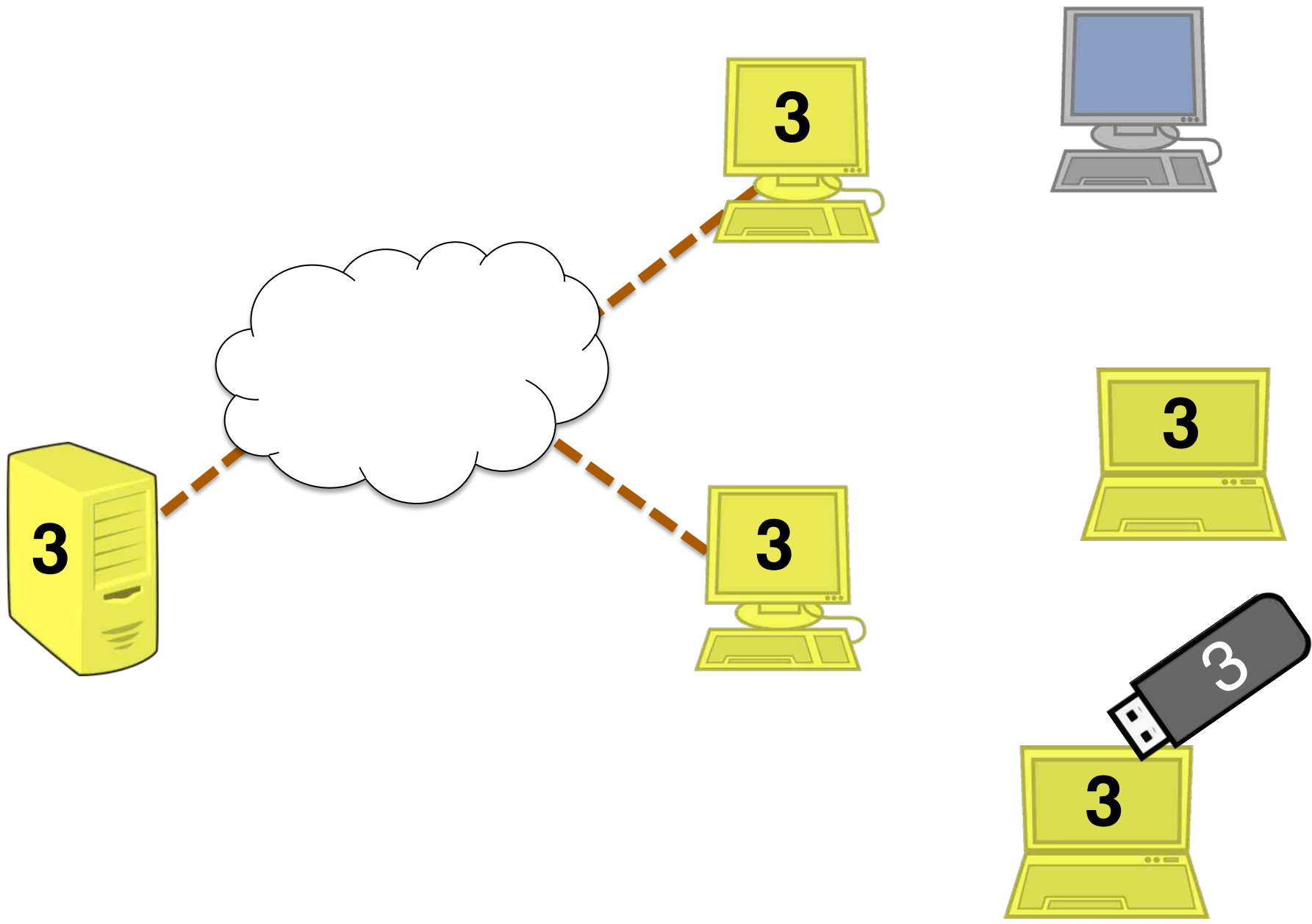










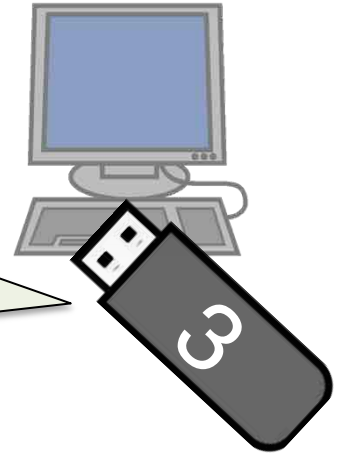


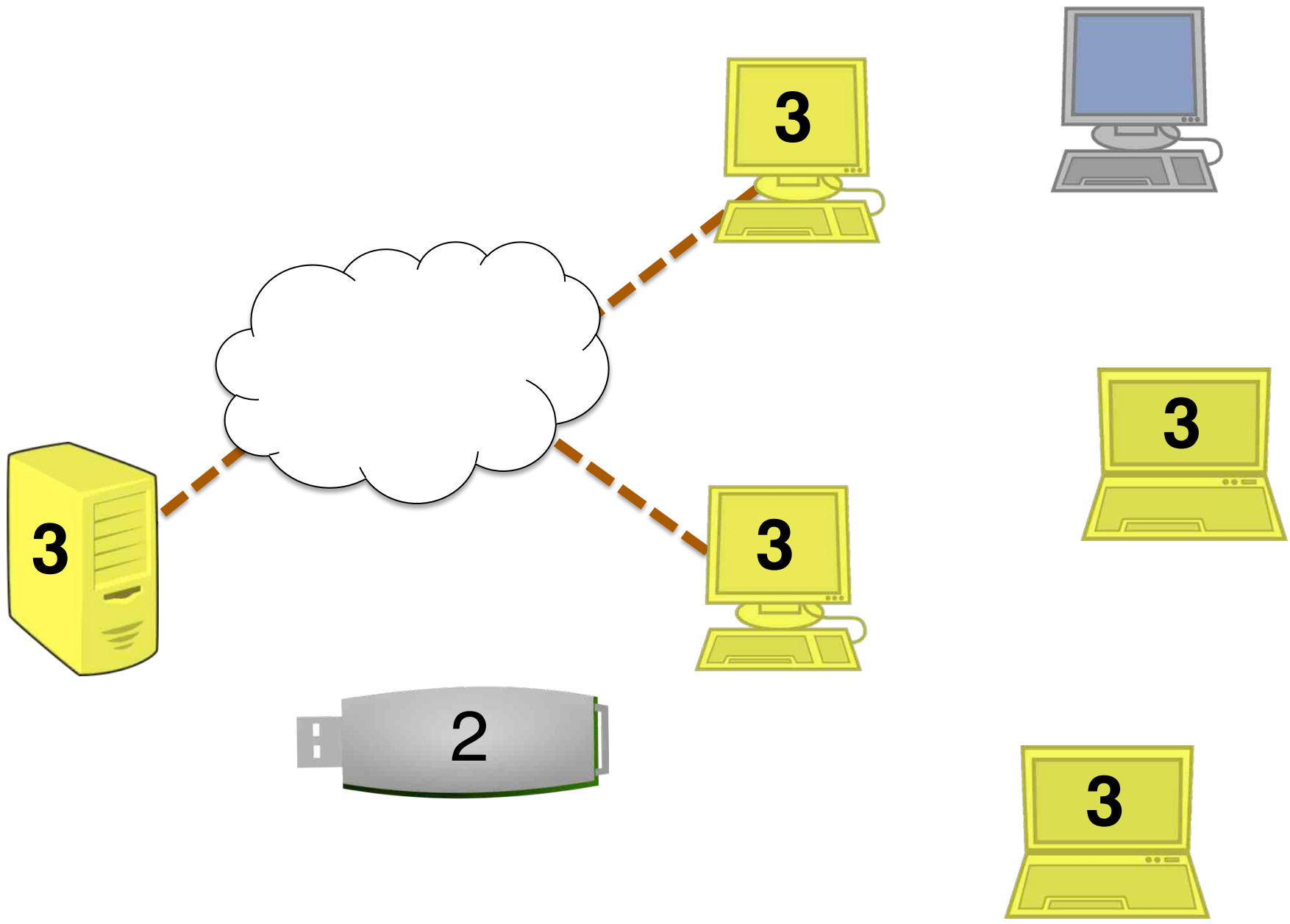
G:\Videos\MJ.mov

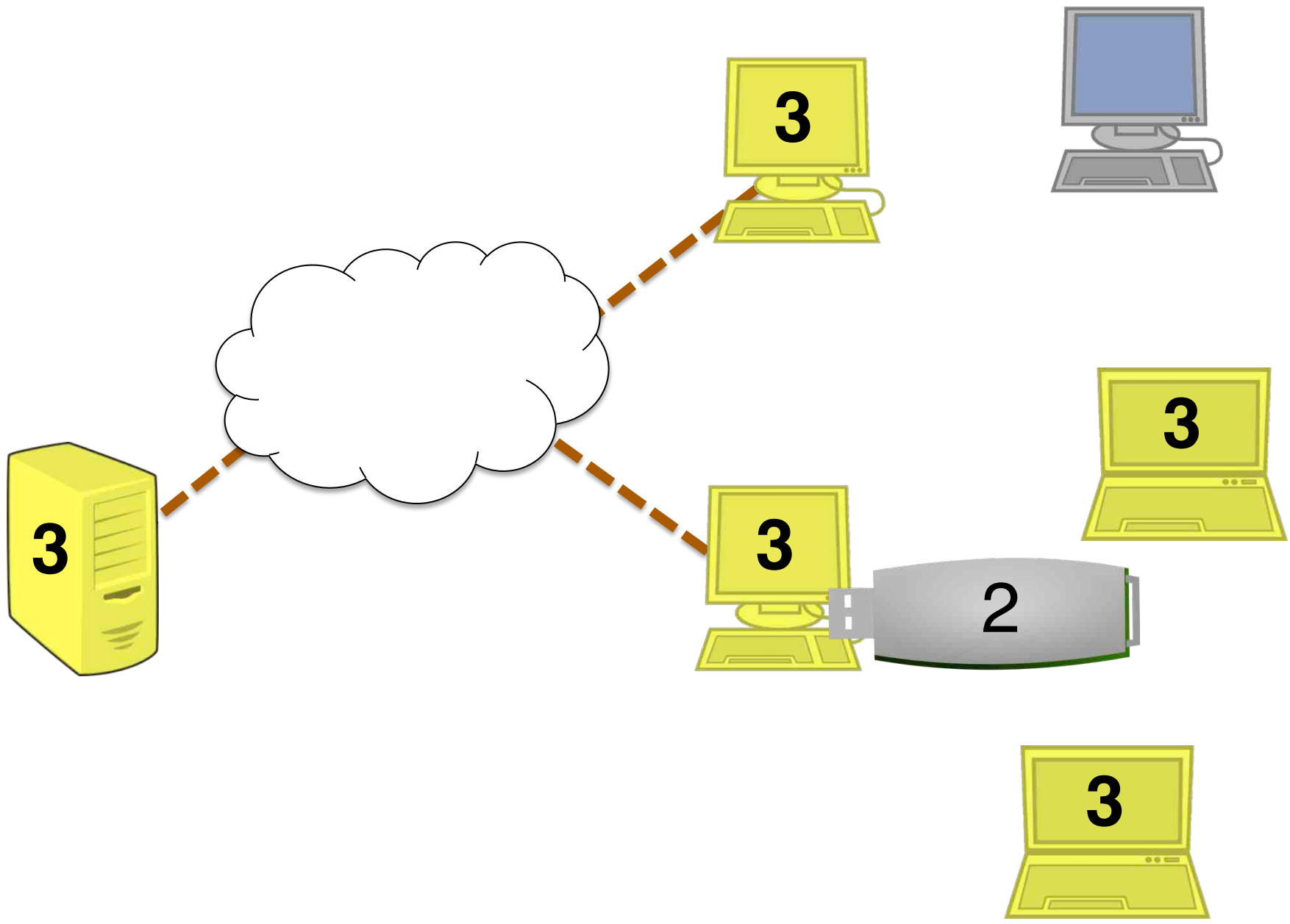
...

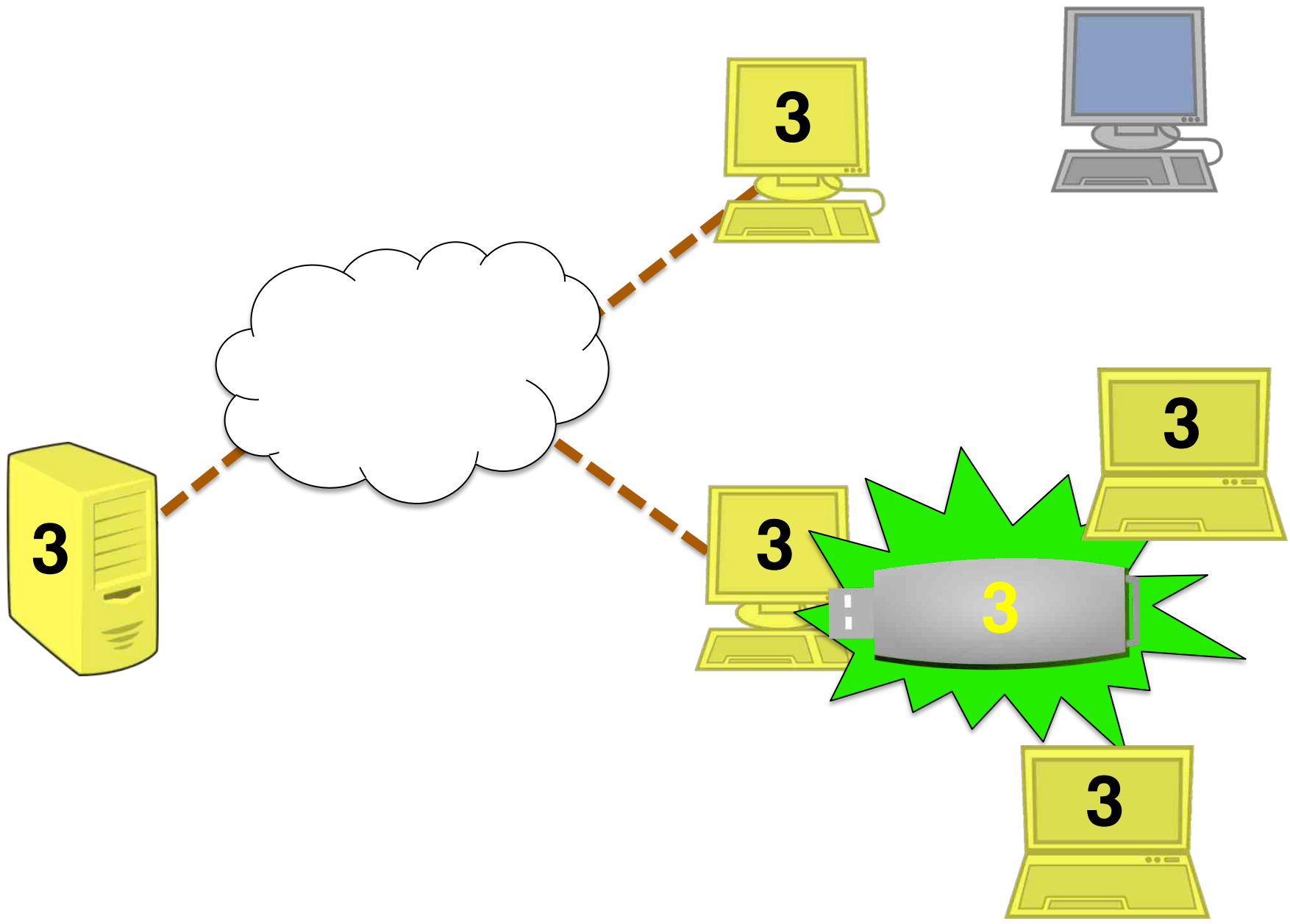
G:\FlashPatch\data.db

G:\FlashPatch\README.txt

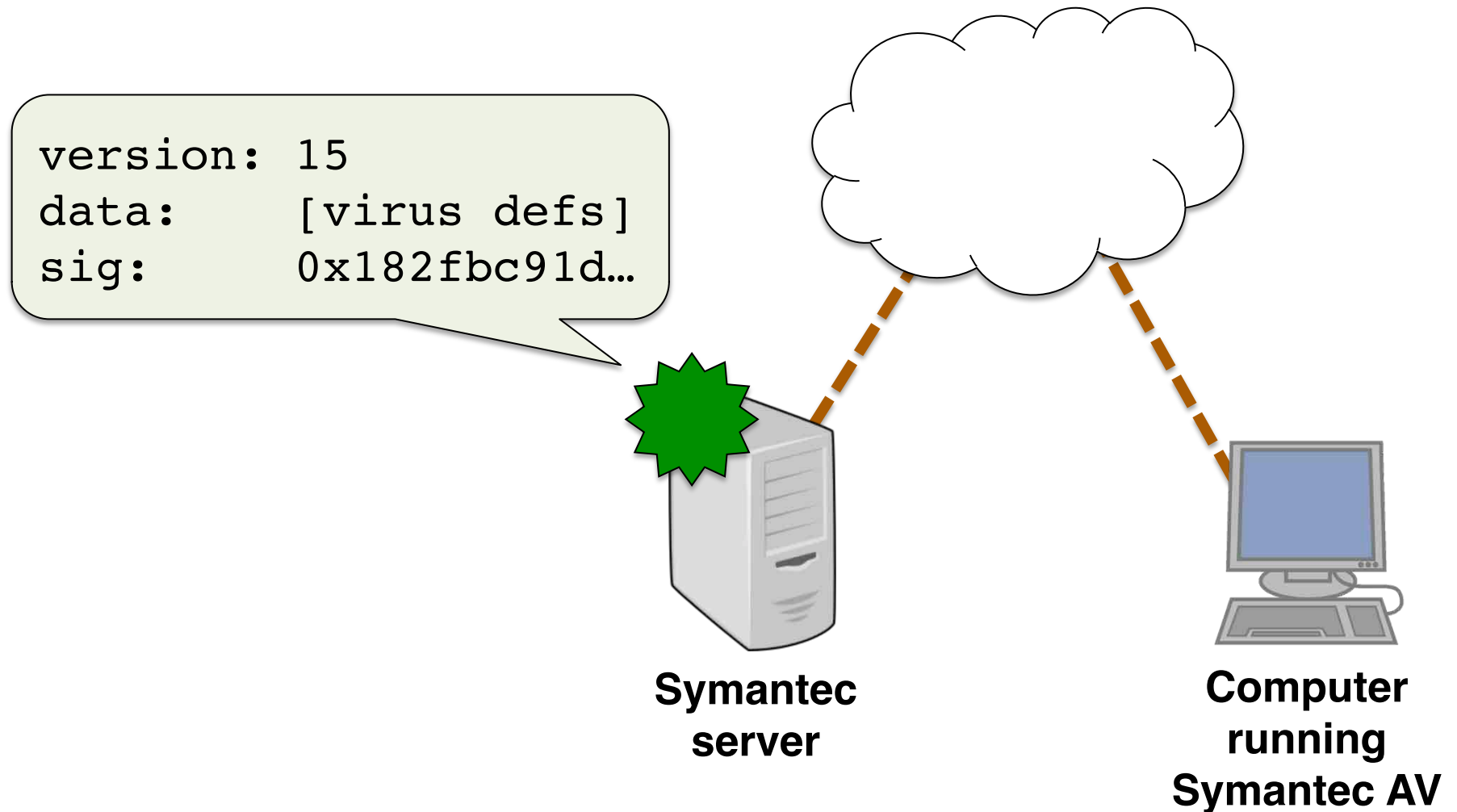








# How it works



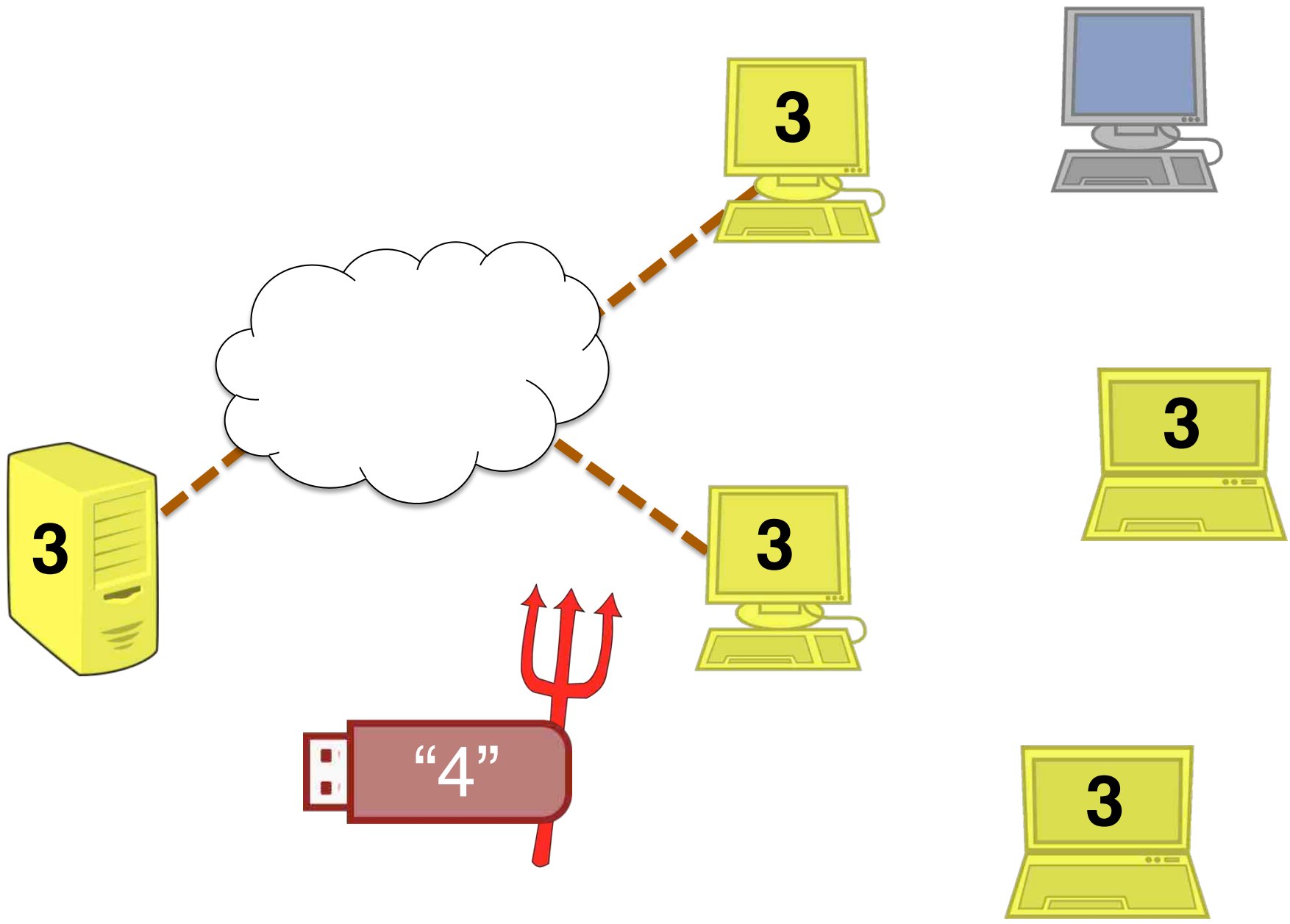
# Properties

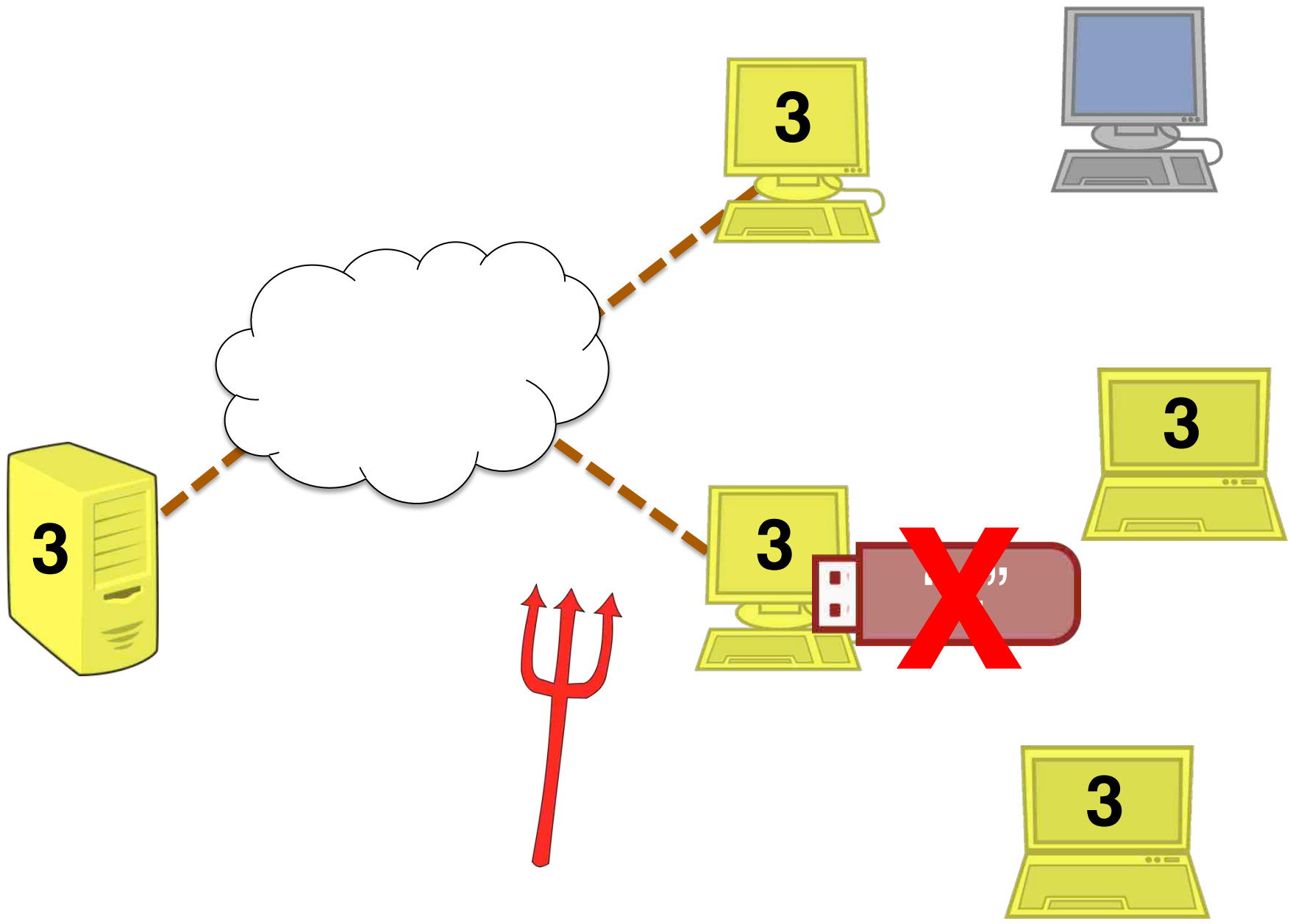
## **Consistency**

Single vendor → No conflicting updates

## **Security**

Digital signatures → No “impostor” updates





# Review: Goals

Build a system for distributing software updates that:

✓ Requires no new hardware

✓ **Runs on JWXPBs** (Junky Windows XP Boxes)

✓ Requires no training

**No user intervention after install**

3. Is more effective than *status quo*



# Outline

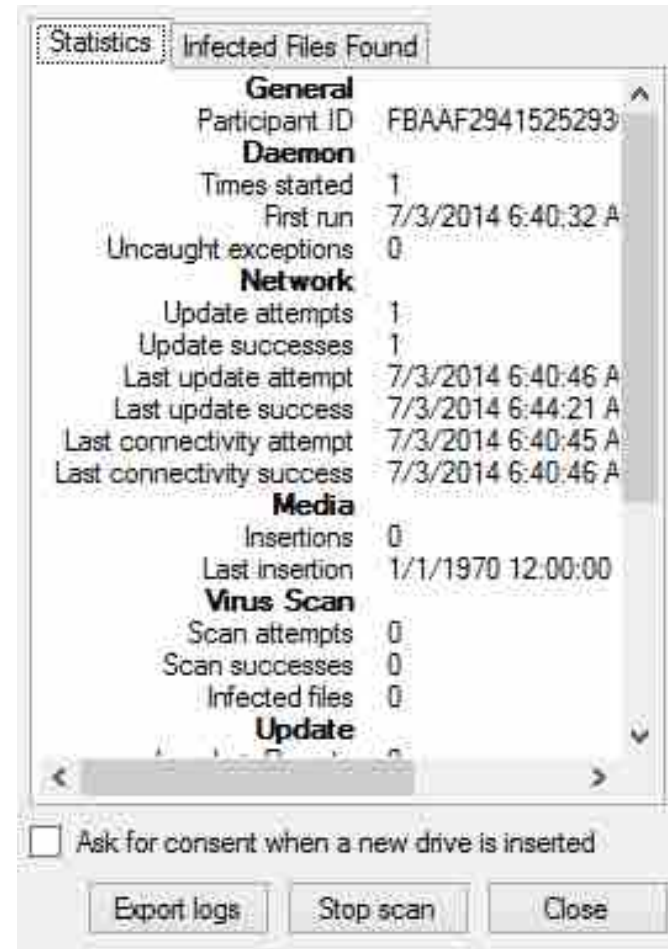
- Motivation
- System design
- **Evaluation**
- Conclusions

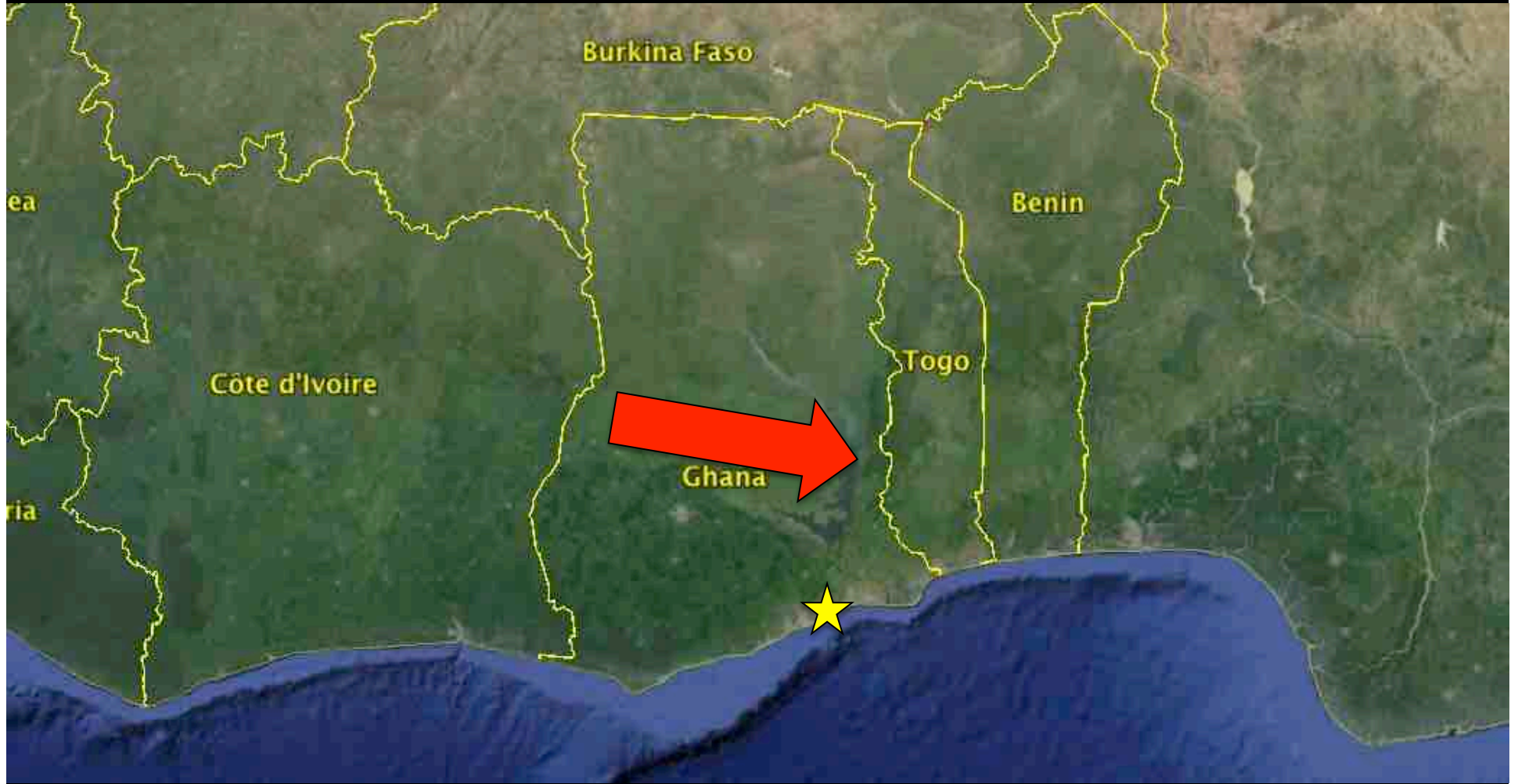
# Research Questions

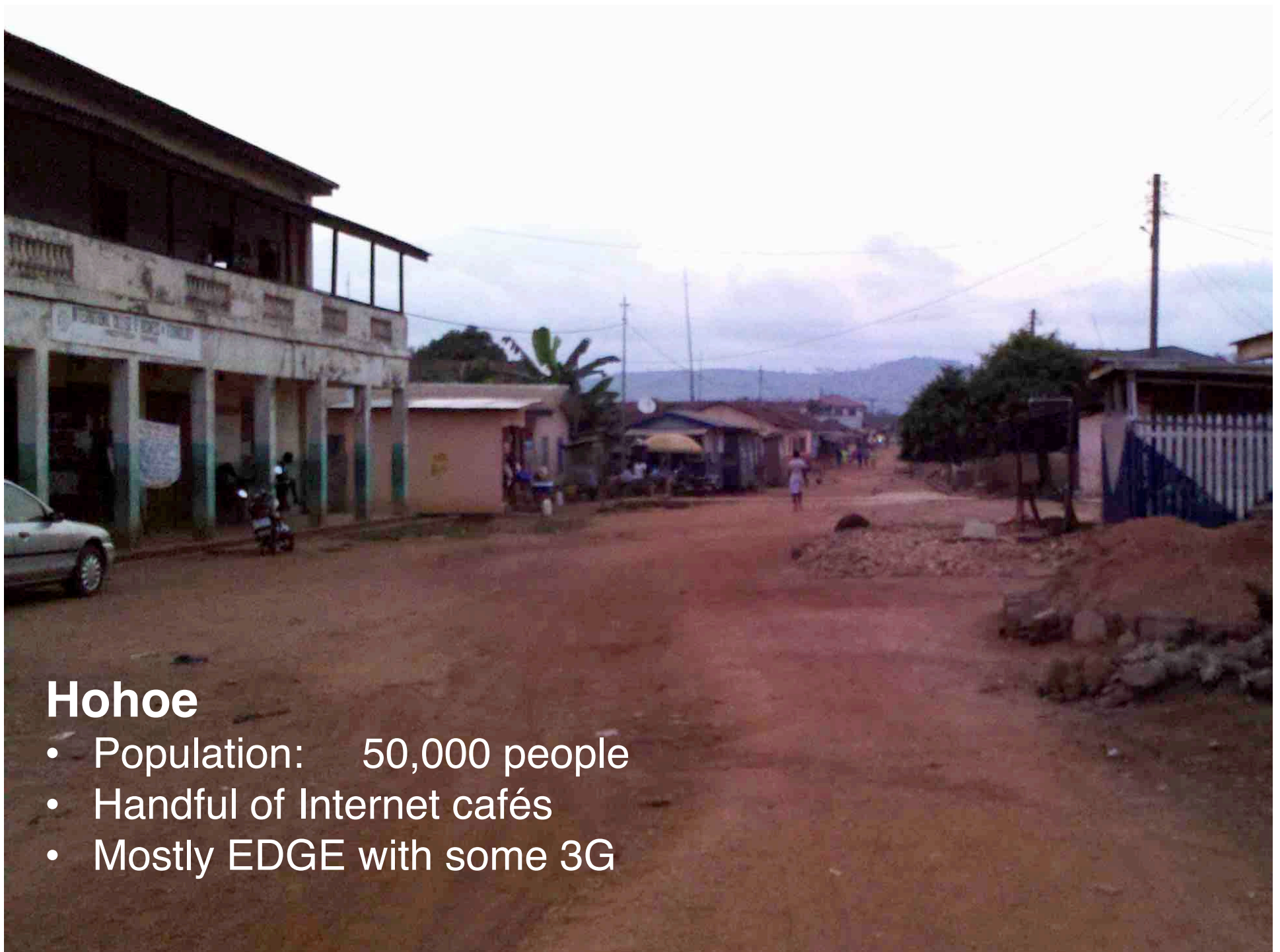
1. How quickly do flash drives move?
2. How prevalent are viruses? Which ones?
3. Is FlashPatch effective?

# Implementation: Virus scanner

- Based on open-source ClamAV
- 3,400 lines of C#
- Spreads DB updates **via FlashPatch**
- Scans all inserted flash drives for viruses
- Sends back “anonymized” log files







## Hohoe

- Population: 50,000 people
- Handful of Internet cafés
- Mostly EDGE with some 3G

# Ethical Considerations

- Informed consent
- Resource use (flash space)
- Limited distribution (we install the daemon)
- Opt out
- Privacy (MACs, IPs, file names)

# Deployment

Deployed at:

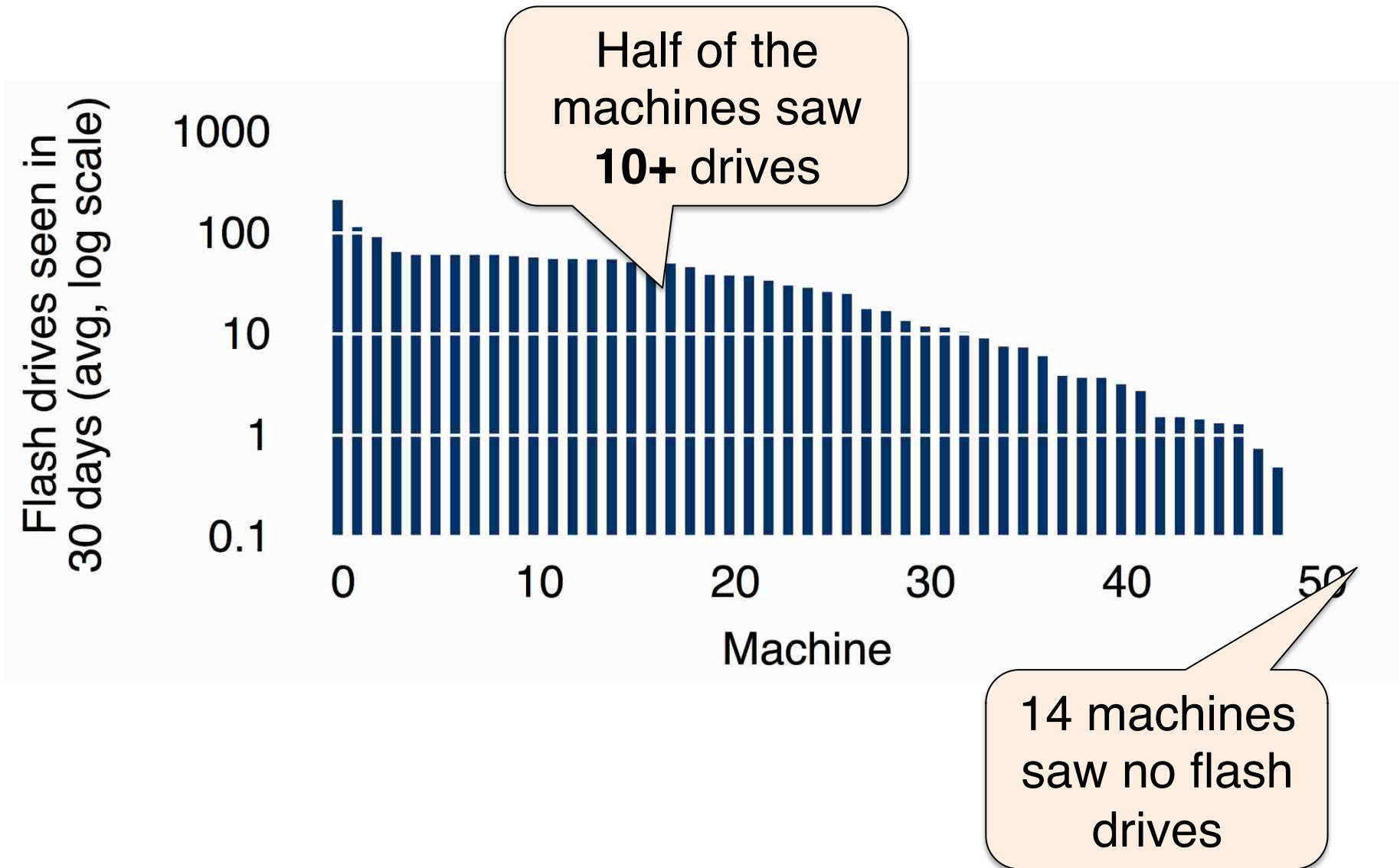
- 6 Internet cafes
- 1 secondary school
- 1 graphic design shop

**63** machines total

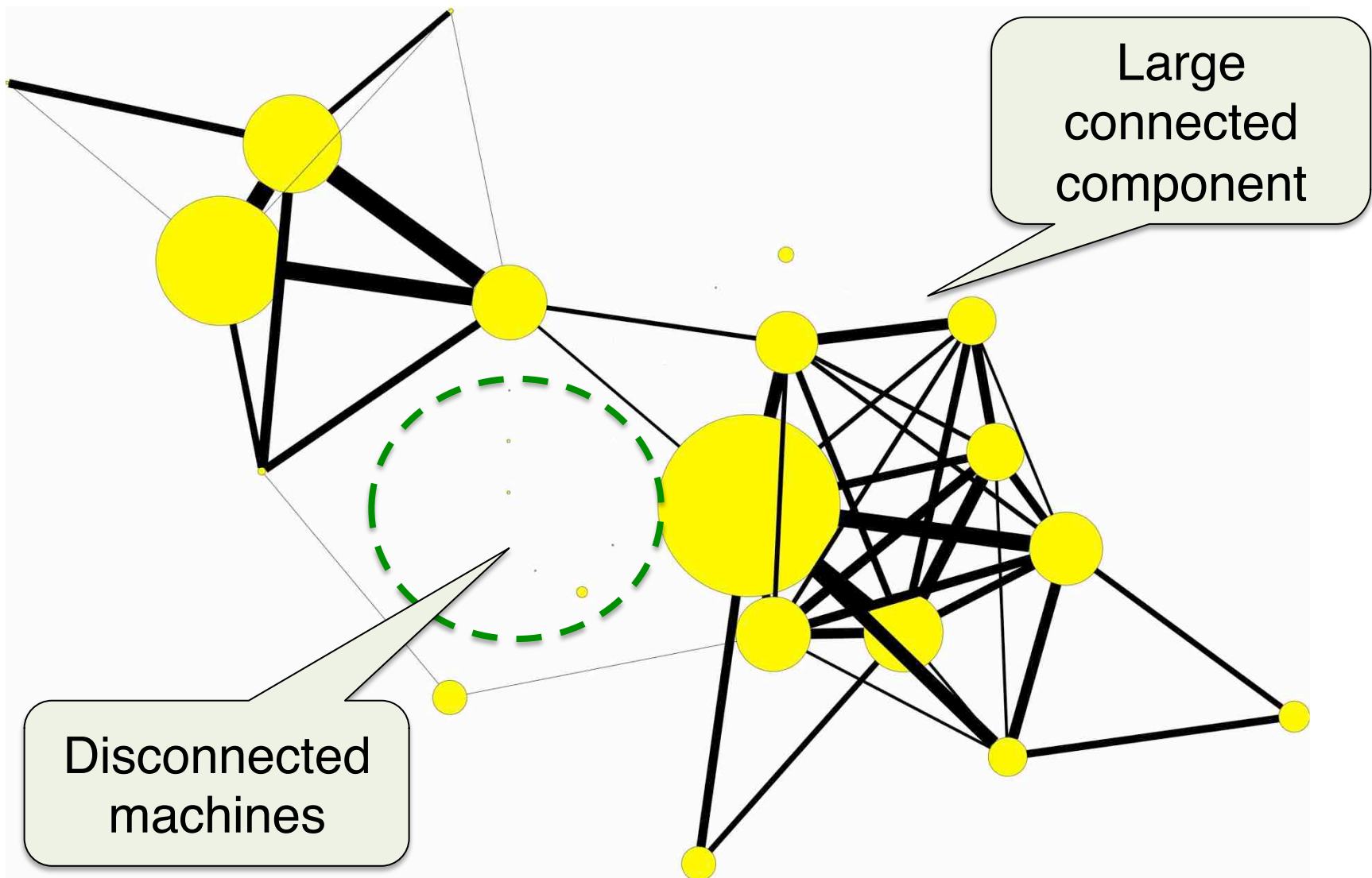


Between July 2013 and March 2014

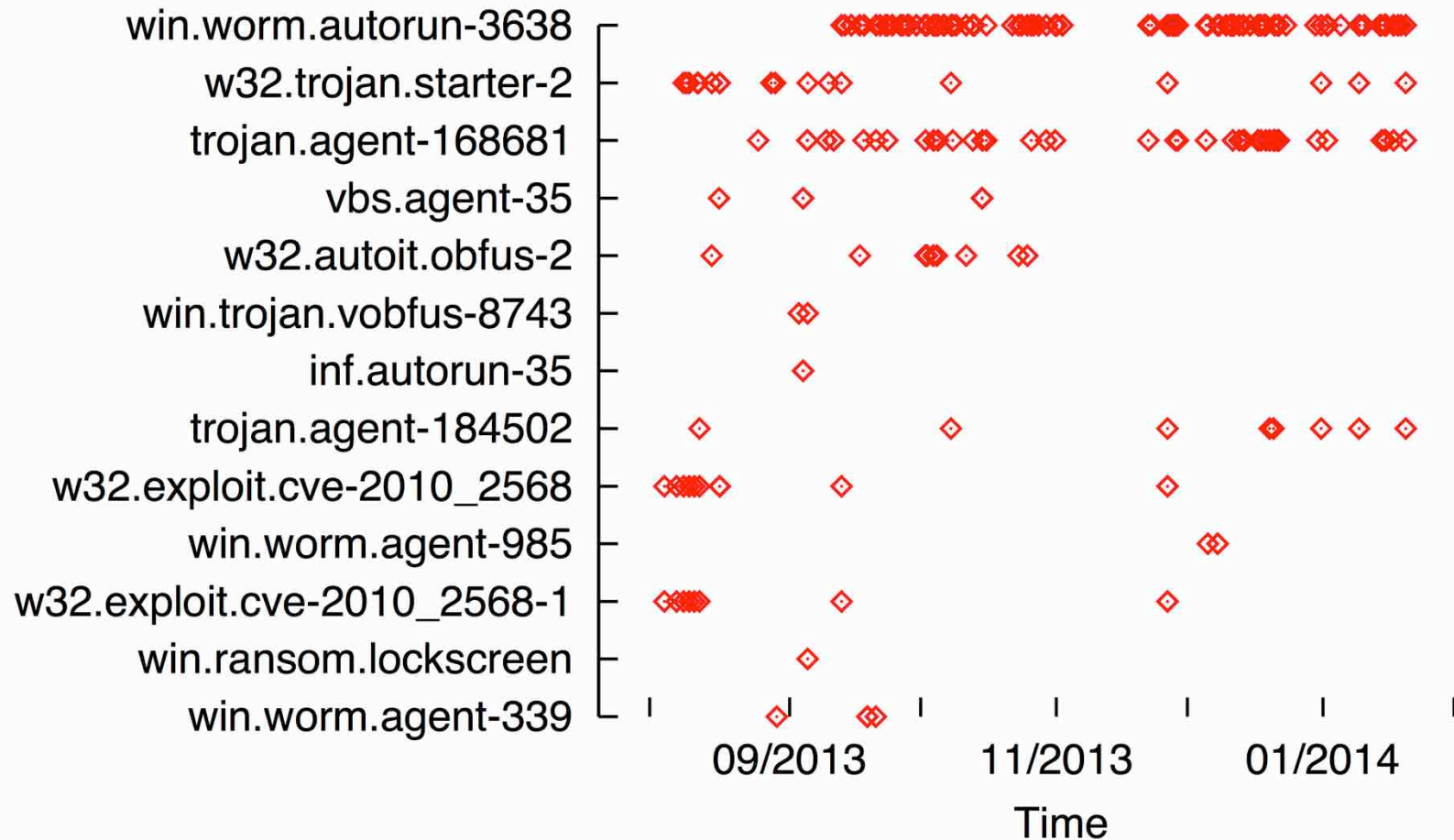
# Q1: How quickly do flash drives move?



# Q1: How quickly do flash drives move?



# Q2: How prevalent are viruses?

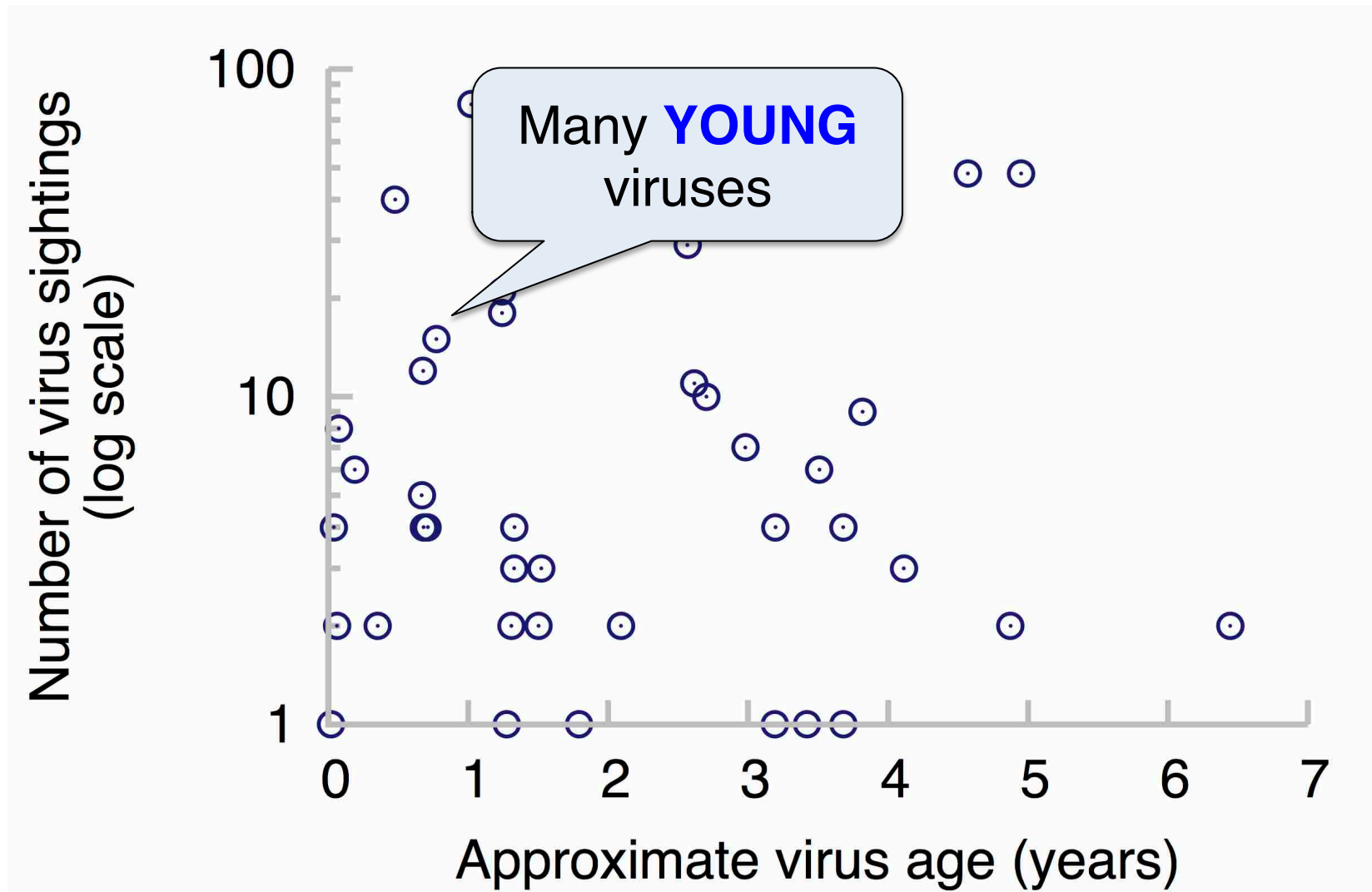


## Q2: How prevalent are viruses?

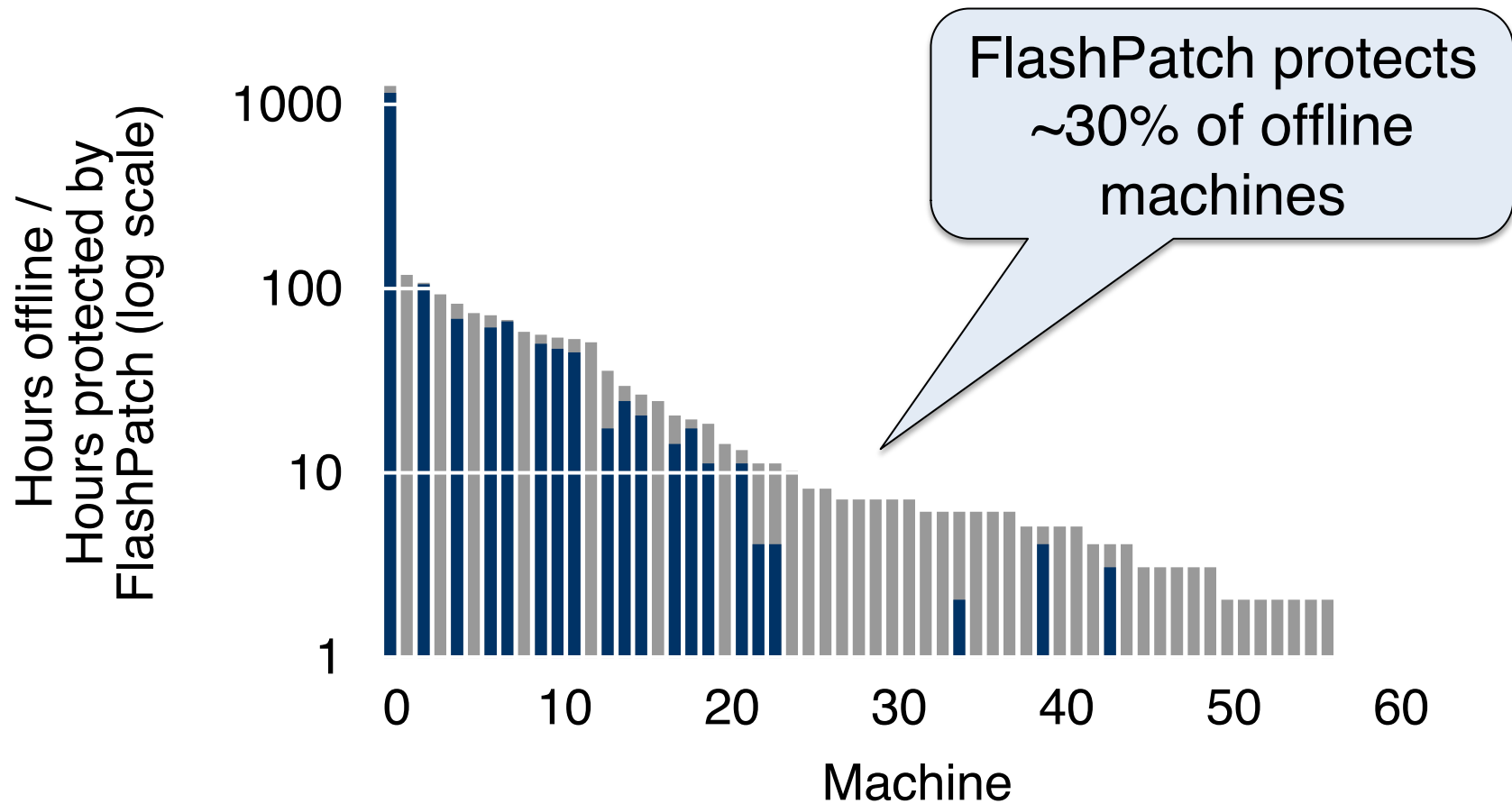
- Scanned 1,242 flash drives
  - **233** had at least one infected file (19%)
  - 10% of drives had 6+ infected files
- 48 distinct virus types
  - Max: 130 sightings
  - Min: 1 sighting

... and ClamAV doesn't catch everything...

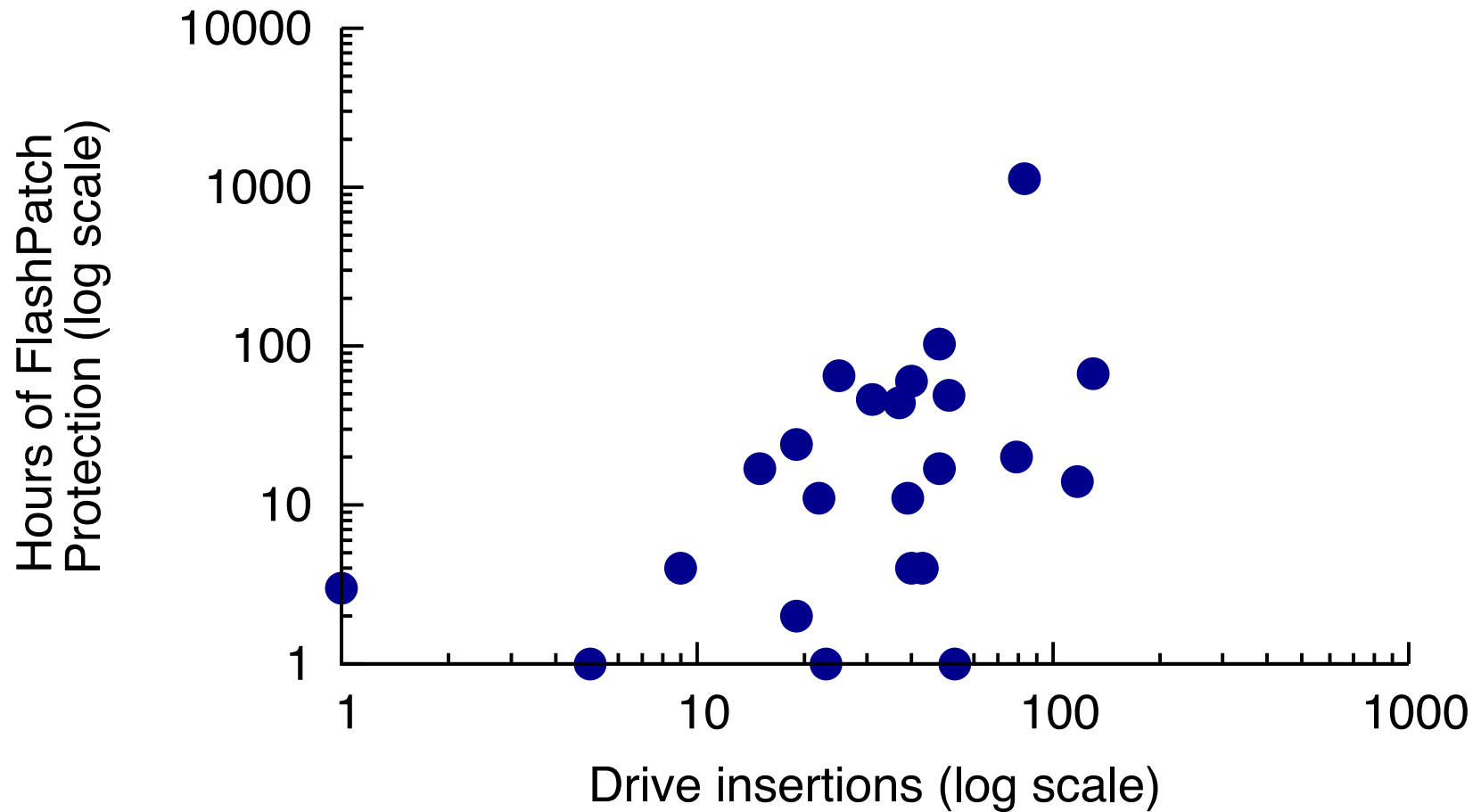
# Q2: How prevalent are viruses?



# Q3: Is FlashPatch effective?



# Q3: Is FlashPatch effective?



# Outline

- Motivation
- System design
- Evaluation
- **Conclusions**

# Final Thoughts

**FlashPatch**: a system for spreading software updates in under-connected regions

- No new hardware
- No training

## What's next

- Could FlashPatch be built into a “real” AV?
- Are there other opportunities for HW-free ICTD?



