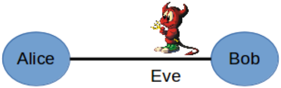
Side-Channel Attacks: Strategies and Defenses

Stefanie Roos

Outline

- What are Side-Channel Attacks (SCAs)?
- Which adversary models are suitable for SCAs?
- Which types of attacks exists?
- How do these attacks work precisely?

Side-Channel Attacks

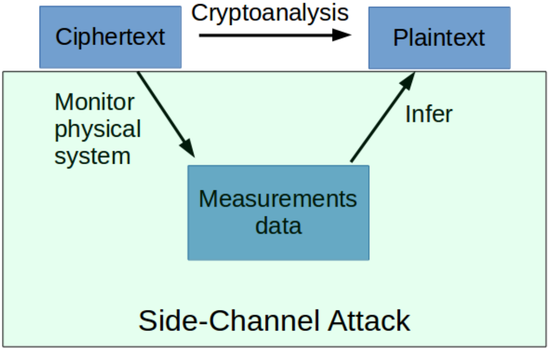


Model

Physical Implementation

- We prove the security of cryptographic algorithms in a mathematical model
- But implement them in the physical world

Side-Channel Attacks (2)



- Side-channel attacks exploit physical properties of an implementation
- Enable an attacker to bypass encryption

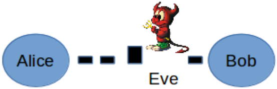
Adversary Models

- What does Alice encrypt?
  - Messages sent via an encrypted connection
  - Data on her own device
  - Data/Computations in the cloud

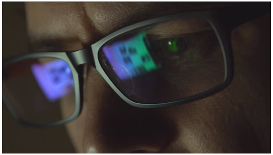
- How much can Eve observe, measure, and control?
  - Router (Internet provider)
  - Visual contact (Surveillance camera)
  - Detailed device measurements (Family member)
  - Controls device (Cloud provider)

Potential Attack Vectors

- Bandwidth consumption



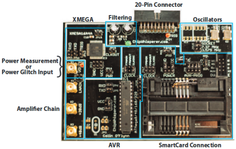
- 'Shoulder-surfing'
- Reflections



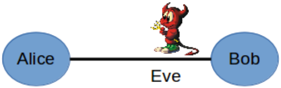
Potential Attack Vectors

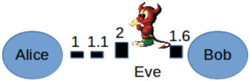
- Timing computations
- Power consumption
- Electromagnetic emission
- Sound emissions

- Cache access
- Differential power analysis
- Differential fault analysis



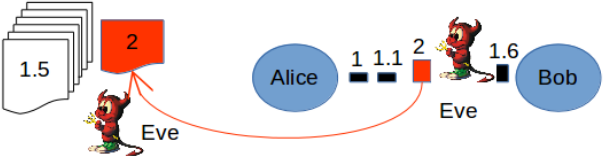
Bandwidth Consumption: Scenario





- Eve observes communication going via Alice's Router
- Alice accesses health forum via encrypted connection
- Eve knows that Alice connects to health forum
- But cannot decrypt downloaded content

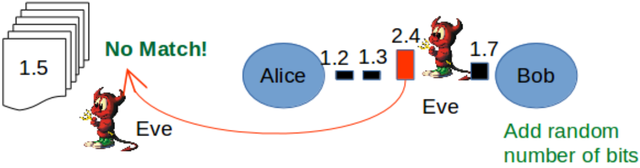
Bandwidth Consumption: Attack



- Eve determines size of all pages on health forum
- Eve measures size of Alice's downloaded pages
- Likely: Eve can uniquely map download to page
- This attack is called *website fingerprinting*

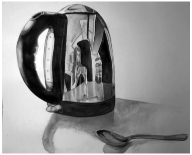
Bandwidth Consumption: Defense

- Pad all pages to common size (inflexible + inefficient ☹)
- Dynamic personalized websites
- (Finally a benefit of targeted advertisement)



Reflections: Scenario

- Alice types her password on a device in a public place
- Alice hides her screen
- But there is a reflecting surface close



Reflections: Attack and Defense

- Eve uses a camera and a telescope
- Off-the-shelf: less than 2,000 C$
- Photograph reflection of screen through telescope
- Reconstruct original image
- Distance: 10–30 m
- Depends on equipment and type of reflecting surface

Literature

- Francois-Xavier Standaert: Introduction to Side-Channel Attacks
- Website Fingerprinting
  - Andrew Hintz: Fingerprinting Websites Using Traffic Analysis, PET 2002
  - Hermann et al.: Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Nave-Bayes Classifier, CCSW 2009
- Reflections
  - Backes et al.: Compromising Reflections-or-How to Read LCD Monitors around the Corner, Security and Privacy 2008
  - Backes et al.: Tempest in a teapot: Compromising reflections revisited, Security and Privacy 2009