Welcome to "Little Bits to Big Ideas"

Lab 11: Security

TAs: Ashish & Shivani

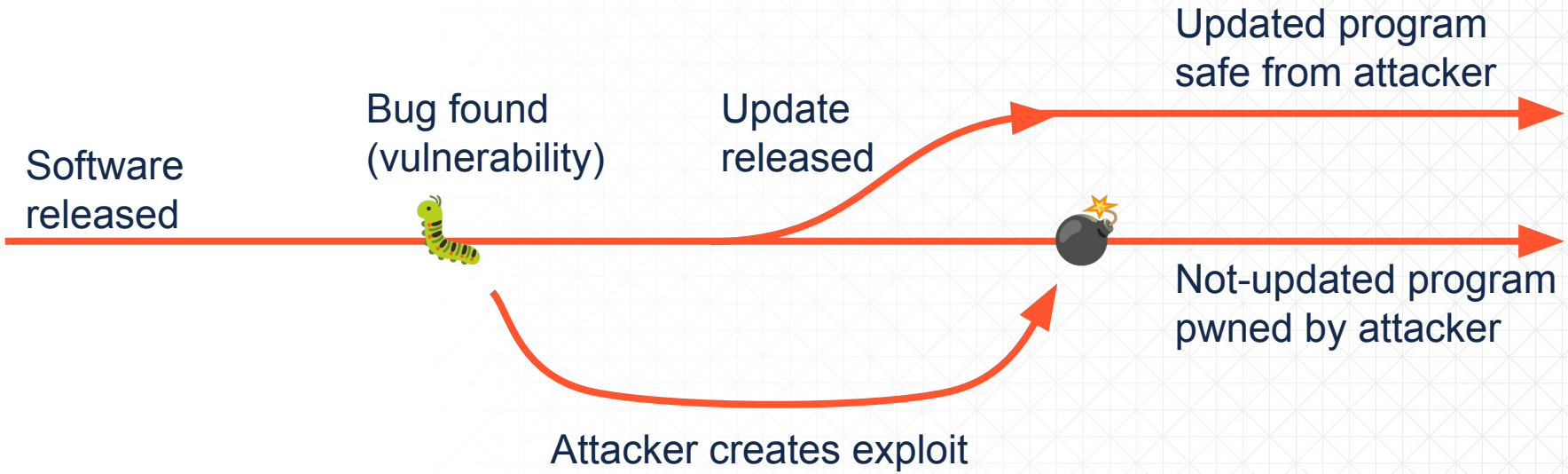
CAs: Abhinav, Harry, & Sherry

ILLINOIS

Two most important rules

- Always apply software updates
- Never reuse a password for multiple sites

Why apply updates?



Why no password reuse?

- Employees of each site you have an account with
  can learn the username and password you use to log in
  and use it to impersonate you on other sites
- Also, if one site is hacked, hackers might learn your password

Secure communication

- **Authentication** establishes **who** is communicating
  - Digital certificates
  - Username and password
- **Confidentiality** ensures others **can’t eavesdrop** on a conversation
  - Symmetric cipher
- **Integrity** ensures that messages are **not modified** in transit
  - Hashes
  - Symmetric cipher

Rights management

- **Authentication** establishes **who** is communicating
- **Authorization** establishes **what** people are allowed to do
- **Principle of least privilege**
  - Each party should only have rights they legitimately need to have
  - Oposite of a “firewall” all-or-nothing model

Lab activity

“Two truths and a lie” with a crypto twist

Part 1: signatures

- Public key - share
- ✅ truth - share with good signature
- ❌ lie - share with bad signature

Part 2: encryption

- Pair with another team
- Key exchange
- ✅ truth - share encrypted

Key exchange (Diffie-Hellman)

Things in orange are never shared!

Team 1	Shared	Team 2
rand1, rand2	rand1	rand3
P = f(rand2, rand1)	P and Q	Q = f(rand3, rand1)
key = f(rand2, Q)		key = f(rand3, P)