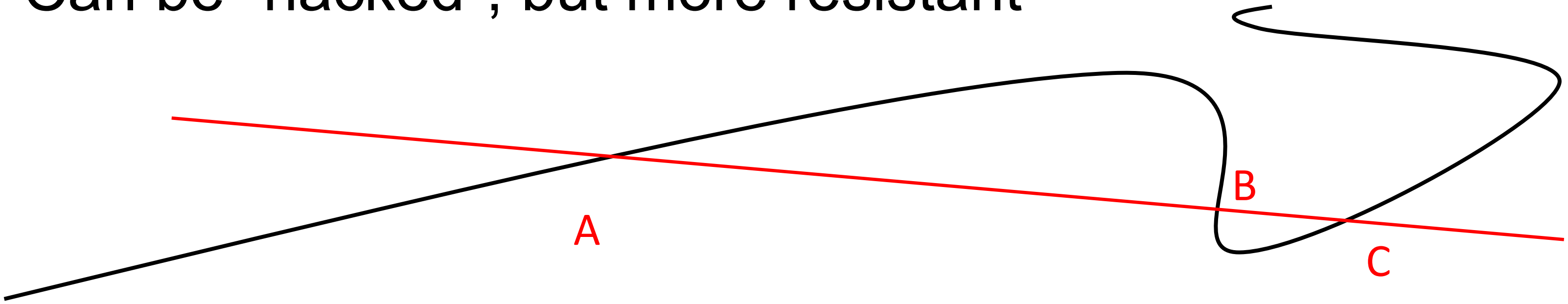
Cybersecurity

Elliptic Curves and Perfect Forward Secrecy

Elliptic Curve Cryptography (ECC)

- Asymmetric encryption
  - Extremely large numbers (integers) that are made from two or more extremely large prime numbers
- ECC uses curves instead of integers
  - Add two points together on a curve to get a third point
  - Can be “hacked”, but more resistant



Traditional web server encryption

- SSL/TLS
  - Uses encryption keys to protect web server communication
  - Traditionally, based on the web server’s RSA key pair
    - One key that encrypts all symmetric keys
- Downfall?
  - This server’s private key
    - Capture all of the data and then decrypt the data
- One single point of failure

Perfect Forward Secrecy (PFS)

- Public key system in which a key derived from another key is not compromised
  - Even if the original key is compromised in the future
- What happens if not in place?
  - All past data that’s been recorded can easily be decrypted

Security Through Obscurity

- Concept that security can be achieved by hiding what is secured
- Not the most valid method of hiding data
- Obscurity makes it harder for a hacker to guess critical pieces
  - Should not be the only thing relied upon though
    - Not the only layer of protection