Some recent research work on security and privacy

Anish Mathuria

August 22, 2017
Secure cloud storage

• Loss of control over data
  – non-traditional threats

• A malicious cloud provider
  – may allow unauthorized users to write data
  – may manipulate the order in which the updates are stored
  – may collude with a writer authorized user to conceal an update
    • Ex: overwriting an original prescription, after the consulting session is over

• Challenges
  – Developing cryptographic techniques for verifying correct operation of the storage system
  – Building secure storage on top of existing cloud providers
Efficient private matching

Similar document detection:
Alice has a document d and wants to know which documents in Bob's collection are similar to d, without revealing d to Bob

Set intersection:
Alice has a test license plate p and wants to know if it is present in the plate database with Bob, without revealing p to Bob

• Known solutions: compute homomorphically
  – in many cases too expensive for applications
• Challenges
  – Making the techniques practical
  – Semantic hashing
Low-level attack techniques

• Shellcode
  – architecture-specific code injected into running programs to exploit security holes
  – automated generators: rix, alpha3
  – Our work
    • to reduce the size expansion of generated shellcodes
    • source code: https://bitbucket.org/mitthu/alpha_loaders/overview

• Port scanning
  – Attackers wish to discover services they can break into
  – Idle (blind) port scan
    • avoid sending any non-spoofed packets to target
  – Our work
    • Eliminating race conditions in RST rate-limit scan
    • Practical demonstration
References

• N. Kumar and A. Mathuria. Improved write access control and improved freshness guarantee to outsourced data. ICDCN’17.


• R. Odhaviya, A. Modi, R. Seth and A. Mathuria. Feasibility of idle port scanning. 10th ACM International Conference on Security of Information and Networks (SIN’17), Accepted.
