



Computer Security

Honeypots, Side-Channel Attacks

Erland Jonsson
Department of Computer Science
and Engineering



Honeypots



Honeypot - definition



Definition :

- Honeypots are **fake computer systems**, setup as a "decoy", that are used to **collect data on intruders**
- This "decoy" appears to contain operating system vulnerabilities that make it an **attractive target for hackers**.
- A honeypot, loaded with fake information, **appears** to the hacker to **be a legitimate machine**.
- While it appears vulnerable to attack, it actually prevents access to valuable data
- It is an example of a **deception system**.

Honeypots - categories



Honeypots are categorized based on their **deployment**:

- **Production honeypots** - normally low-interaction honeypots with the intention to reduce risk in an organisation
- **Research honeypots** - gather information about the motives and tactics of the attackers. They are complex to deploy and maintain. They capture extensive information

or with respect to the **level of interaction** they have with the attackers:

- **low-interaction** - simulates the services that the attackers are normally asking for. Low resource-demanding, fast response
- **high-interaction** - offers most of the services of a system. Expensive to maintain. Difficult to detect.

Honeynet



- A honeynet is a **network of honeypots**
- The purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security can be gathered
- Results from the nodes in the honeynet can be **analysed in a central node**
- The advantage with a honeynet is that distributed attacks and low-interference (stealth) attacks can be studied

Side-channel Attacks



Side-channel attacks

- A **side channel attack** is any attack based on information gained from the **physical implementation of a cryptosystem**
- It normally requires **physical access** to the hardware
- A side-channel attack is an attack based on **side-channel information**, i.e. “extra” information that can be retrieved from a crypto device and that is neither plaintext or the ciphertext

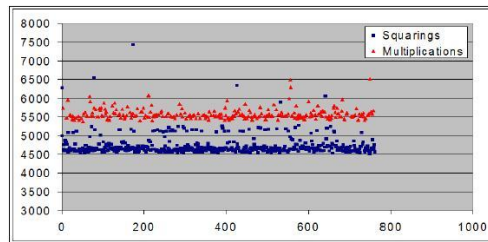


Fig. 9. Best result of our SBPA against OpenSSL RSA, yielding 508 out of 512 secret key bits.

Side-channel attacks

- Types of side-channel attacks:
 - **Timing attack** – attacks based on measuring **how much time various computations take** to perform.
 - **Power monitoring attack** - attacks based on observing the **varying power consumption** by the hardware during computation
 - **Electromagnetic attacks** – based on observing **electromagnetic emanation**, cp. TEMPEST (Sw. RÖjande Strålning = RÖS)
 - **Acoustic cryptanalysis** - attacks which **exploit the sound produced** during a computation
 - **Differential fault analysis** - in which secrets are discovered by introducing faults in a computation.

