Practical Aspects of Modern Cryptography

Winter 2011

Josh Benaloh
Brian LaMacchia

Side-Channel Attacks

Breaking a cryptosystem is a frontal attack, but there may be easier access though a side or back door – especially on embedded cryptographic devices such as SmartCards and RFIDs.

Side-Channel Attacks

Some attack vectors …

Side-Channel Attacks

Some attack vectors …

- Fault Attacks

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks
- Power Analysis

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks
- Power Analysis
- Electromagnetic Emissions

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks
- Power Analysis
- Electromagnetic Emissions
- Acoustic Emissions

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks
- Power Analysis
- Electromagnetic Emissions
- Acoustic Emissions
- Information Disclosure

Side-Channel Attacks

Some attack vectors …

- Fault Attacks
- Timing Attacks
- Cache Attacks
- Power Analysis
- Electromagnetic Emissions
- Acoustic Emissions
- Information Disclosure
- … others?

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

- Heat

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

- Heat
- Cold

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

- Heat
- Cold
- Low power

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

- Heat
- Cold
- Low power
- Microwaves

Fault Attacks

(N.B. Problem 3 of Assignment 1 where a mod Q error in RSA decryption/signatures discloses key.)

Faults may be unintentional or induced by …

- Heat
- Cold
- Low power
- Microwaves
- …etc.

Timing Attacks

How long does it take to perform a decryption?

Timing Attacks

How long does it take to perform a decryption?

The answer may be data-dependent.

Timing Attacks

How long does it take to perform a decryption?

The answer may be data-dependent.

For instance…

Timing Attacks

How long does it take to perform a decryption?

The answer may be data-dependent.

For instance…

- $N = PQ$

Timing Attacks

How long does it take to perform a decryption?

The answer may be data-dependent.

For instance…

- $N = PQ$
- Watch decryption times for $z = E(m)$ where $m < P$ and where $m > P$.

Timing Attacks

How long does it take to perform a decryption?

The answer may be data-dependent.

For instance…

- $N = PQ$
- Watch decryption times for $z = E(m)$ where $m < P$ and where $m > P$.
- If there is a minute difference, P can be determined with binary search.

Cache Attacks

If you can run code on the same device where a decryption is being performed, you may be able to selectively force certain cache lines to be flushed.

Cache Attacks

If you can run code on the same device where a decryption is being performed, you may be able to selectively force certain cache lines to be flushed.

Decryption times may vary in a key-dependent manner based upon which lines have been flushed.

Power Analysis

Power usage of a device may vary in a key-dependent manner.

Power Analysis

Power usage of a device may vary in a key-dependent manner.

Careful measurement and analysis of power consumption can be used to determine the key.

Electromagnetic Emissions

One can record electromagnetic emissions of a device – often at a distance.

Electromagnetic Emissions

One can record electromagnetic emissions of a device – often at a distance.

Careful analysis of the emissions may reveal a secret key.

Acoustic Emissions

Modular exponentiation is using done with repeated squaring and conditional "side" multiplications.

Acoustic Emissions

Modular exponentiation is using done with repeated squaring and conditional “side” multiplications.

It can actually be possible to hear whether or not these conditional multiplications are performed.

Information Disclosures

(N.B. Bleichenbacher Attack)

Information Disclosures

(N.B. Bleichenbacher Attack)

A protocol may respond differently to properly and improperly formed data.

Information Disclosures

(N.B. Bleichenbacher Attack)

A protocol may respond differently to properly and improperly formed data.

Careful manipulation of data may elicit responses which disclose information about a desired key or decryption value.

Certificate Revocation

Certificate Revocation

- Every “reasonable” certification should include an expiration.

Certificate Revocation

- Every “reasonable” certification should include an expiration.
- It is sometimes necessary to “revoke” a certificate before it expires.

Certificate Revocation

Reasons for revocation …

Certificate Revocation

Reasons for revocation …

- Key Compromise

Certificate Revocation

Reasons for revocation …

- Key Compromise
- False Issuance

Certificate Revocation

Reasons for revocation …

- Key Compromise
- False Issuance
- Role Modification

Certificate Revocation

Two primary mechanisms …

Certificate Revocation

Two primary mechanisms …

- Certificate Revocation Lists (CRLs)

Certificate Revocation

Two primary mechanisms …

- Certificate Revocation Lists (CRLs)
- Online Certificate Status Protocol (OCSP)

Certificate Revocation Lists

- A CA revokes a certificate by placing the its identifying serial number on its Certificate Revocation List (CRL)
  - Every CA issues CRLs to cancel out issued certs
  - A CRL is like anti-matter – when it comes into contact with a certificate it lists it cancels out the certificate
  - Think "1970s-style credit-card blacklist"
- Relying parties are expected to check the most recent CRLs before they rely on a certificate
  - "The cert is valid unless you hear something telling you otherwise"

The Problem with CRLs

Blacklists have numerous problems

- They can grow very large because certs cannot be removed until they expire.
- They are not issued frequently enough to be effective against a serious attack.
- Their size can make them expensive to distribute (especially on low-bandwidth channels).
- They are vulnerable to simple DOS attacks.
(What do you do if you can’t get the current CRL?)

More Problems with CRLs

Poor CRL design has made the problem worse.

- CRLs can contain retroactive invalidity dates

  A CRL issued today can say a cert was invalid as of last week.

  - Checking that something was valid at time *t* wasn't sufficient!
  - Back-dated CRLs can appear at any time in the future.
- CAs can even change the CRL rules retroactively.

Yet More Problems with CRLs

- Revoking a cert used by a CA to issue other certs is even harder since this may invalidate an entire set of certs.
- “Self-signed” certificates are often used as a syntactic convenience. Is it meaningful for a cert to revoke itself?

Even More Problems with CRLs

- CRLs can’t be revoked.

  If a cert has been mistakenly revoked, the revocation can’t be reversed.

- CRLs can’t be updated.

  There’s no mechanism to issue a new CRL to relying parties early – even if there’s an urgent need to issue new revocations.

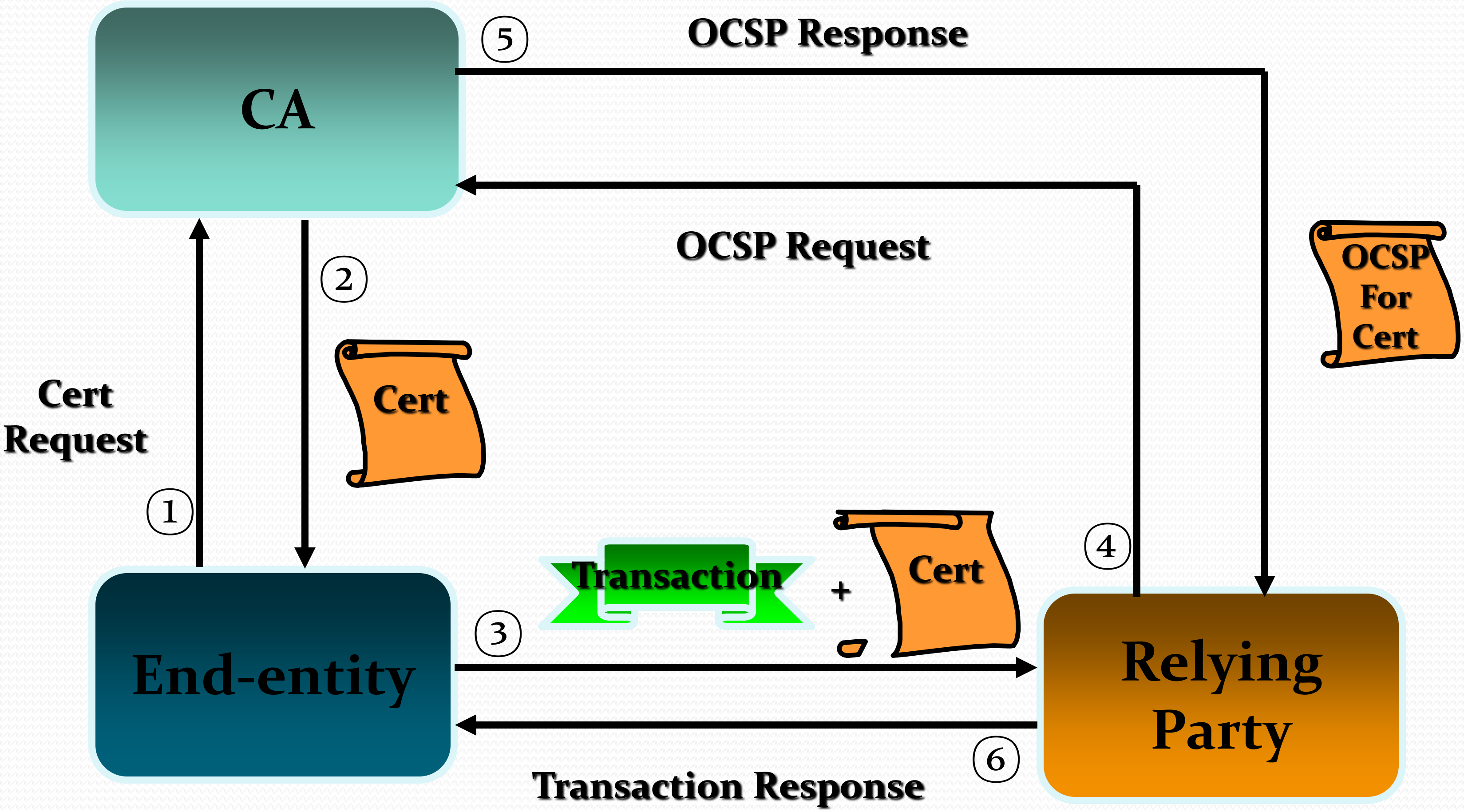
Short-Lived Certificates

If you need to go to a CA to get a fresh CRL, why not just go to a CA to get a fresh cert?

Online Status Checking

- OCSP: Online Certificate Status Protocol
  - A way to ask "is this certificate good right now?
  - Get back a signed response from the OCSP server saying, "Yes, cert C is good at time t"
    - Response is like a "freshness certificate"
- OCSP response is like a selective CRL
  - Client indicates the certs for which he wants status information
  - OCSP responder dynamically creates a lightweight CRL-like response for those certs

OCSP in Action



Final thoughts on Revocation

- From a financial standpoint, it’s the revocation data that is valuable, not the issued certificate itself.
  - For high-valued financial transactions, seller wants to know your cert is good right now.
  - This is similar to credit cards, where the merchant wants the card authorized “right now” at the point-of-sale.
- Card authorizations transfer risk from merchant to bank – thus they’re worth $$$.

Design Charrette

How would you design a transit fare card system?

Fare Card System Elements

- An RFID card for each rider
- Readers on each vehicle and/or transit station (Internet connected?)
- Card purchase/payment machines
- A web portal for riders to manage and/or enrich their cards