Is Your Mobile Device Radiating Keys?

Benjamin Jun
Gary Kenworthy

CRYPTOGRAPHY RESEARCH
a division of Rambus

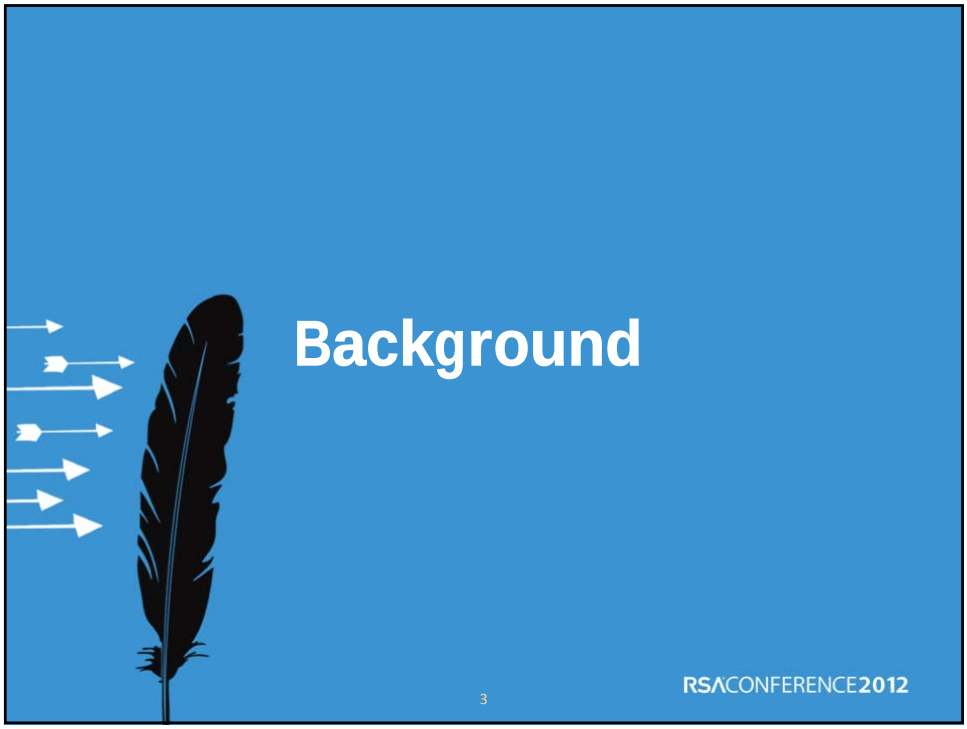
Session ID: MBS-401
Session Classification: Intermediate

RSACONFERENCE2012

Radiated Leakage

- You have probably heard of this before…

- Example of receiving radiated information
  - *without even trying*
- What kinds of secret information might be leaking from your mobile device?

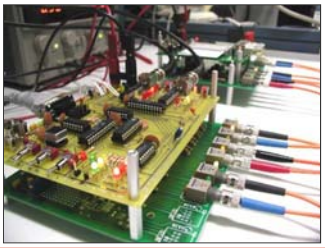


History of Electro-Magnetic (EM) Analysis

- Early work on EM Analysis was classified
  - TEMPEST: Transient electromagnetic pulse emanation standard
- Parts of TEMPEST literature declassified Jan '01 under FOIA .
  - http://www.cryptome.org.
  - Electromagnetic, electrical, acoustic ....
- Relevant TEMPEST literature:
  - NACSIM 5000 tempest fundamentals.
  - NACSEM 5112 NONSTOP evaluation techniques.
  - NSTISSI no. 7000 TEMPEST countermeasures for facilities.

Power Analysis

- Discovered by Cryptography Research in mid-1990s
  - Power consumption of a device leaks information
- Simple Power Analysis (SPA) and Differential Power Analysis (DPA)
  - Low cost, non-invasive attacks on cryptographic implementations
  - Analyzing power consumption reveals the key
- All cryptographic algorithms vulnerable
  - Symmetric crypto: DES, AES, HMAC,…
  - Asymmetric crypto: RSA, DH, EC variants,…
- Affects all types of hardware and software implementations, including:
  - ASICs, FPGAs, smart cards, smart phones,…
- Same techniques work for different side-channels such as EM and RF emissions



Differential Power Analysis

Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
607 Market Street, 5th Floor
San Francisco, CA 94105, USA
http://www.cryptography.com
E-mail: {paul,josh,ben}@cryptography.com

Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

Keywords: differential power analysis, DPA, SPA, cryptanalysis, DES

Background

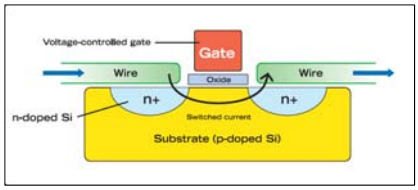
Advances in Cryptology – Crypto 99 Proceedings, LNCS 1666, Springer-Verlag, 1999

CRYPTOGRAPHY RESEARCH a division of Rambus

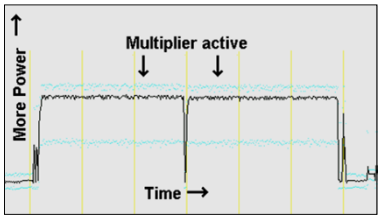
RSACONFERENCE2012

How side channel analysis works

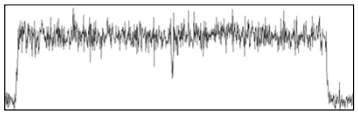
Integrated circuits contain transistors, which consume electricity as they operate. The total power consumption of an integrated circuit and its EM emissions depend on the activity of its individual transistors.



NMOS (N-Channel) Transistor



Power Consumption (RSA operation)



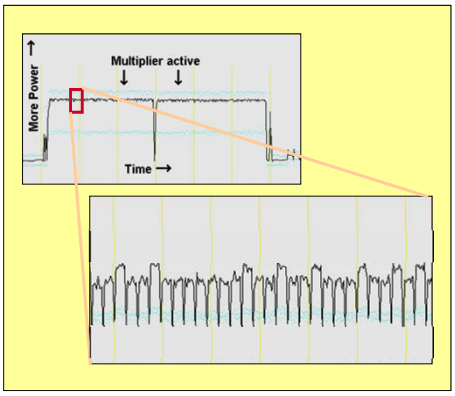
EM emission (RSA operation)

CRYPTOGRAPHY RESEARCH a division of Rambus

RSACONFERENCE2012

Simple Power Analysis (SPA)

- Keys can be extracted from a single trace



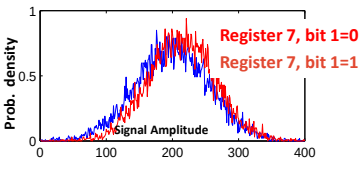
Example RSA Implementation

```
For each bit i of secret d
   perform "Square"
   if (bit i == 1)
      perform "Multiply"
   endif
endfor
```

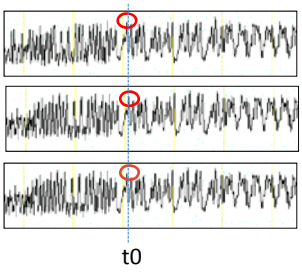
- Similar analysis also applies to EM

DPA: Statistical techniques for analyzing data with low signal/noise ratios

- Signal / noise ratio may be very small
  - However, statistical influence remains…



Power signal amplitude at time t0

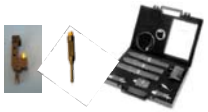


  - Eg. At time t0, mean of signals where register 7 bit 1= 0 is different from mean of signals where register 7 bit 0 = 0

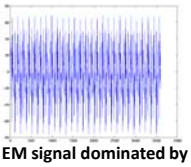
- DPA: Using statistical methods to analyze minute differences in power measurements due to the data being manipulated
- Similar analysis applies to EM measurements

EM Analysis – Early published results

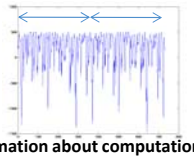
- J.-J. Quisquater & David Samyde E-smart 2001
  - Using m-field probes
- Gemplus: CHES 2001
  - Carefully positioned E and M-field probes on chip surface to isolate signals.
  - Best results required "decapsulating" the chip
  - SEMA and DEMA
- IBM: CHES 2002
  - Used antennas, E and M-field probes
  - Use of receivers, demodulation and signal processing allowed SEMA/DEMA from a distance



near field probes



raw EM signal dominated by clock



Information about computation available after AM-demodulation

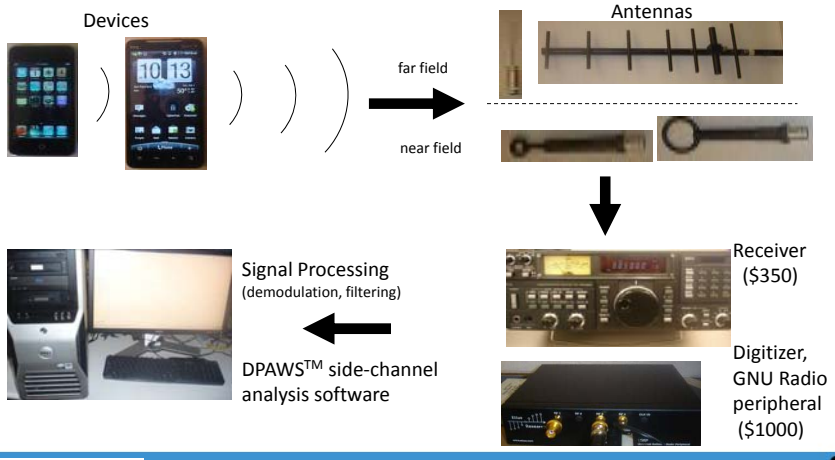
Demonstrations

Overview

- Increased usage of cryptography in smart-phones
  - Payments, encrypted storage, VPNs, SSL, content protection, etc
  - Security requirements in financial, enterprise, govt (FIPS), content space
- CPUs in smart-phones emit electromagnetic (EM) radiation during data processing
  - Emissions contain information about data being processed
- Side-channel analysis of smart-phone emissions reveal secrets and cryptographic keys being used
  - Attacks possible from a few inches to several feet away
  - Applications and OS libraries using crypto are vulnerable

Capturing EM from PDA's/Smartphones

- Simple EM attack with a radio
- Usable signals even at 10 feet away

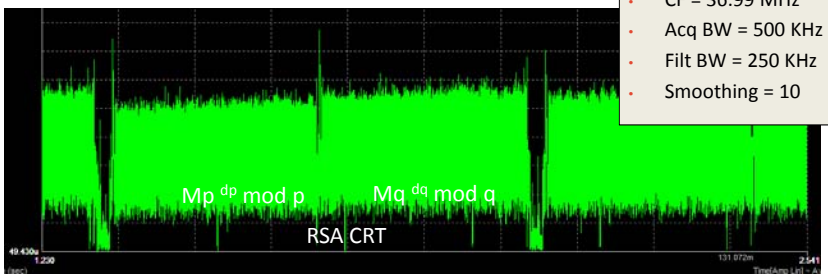


App security Demo 1: M-field attack on RSA

- Android app with simple RSA CRT implementation on HTC Evo 4G phone
- Magnetic field pickup coil placed behind phone
- Measurements collected during computation of

  $M^d \bmod N$

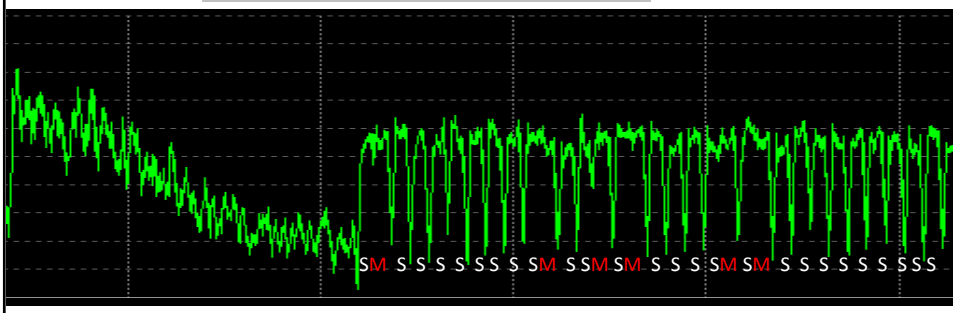
- CF = 36.99 MHz
- Acq BW = 500 KHz
- Filt BW = 250 KHz
- Smoothing = 10



RSA: Key extraction

- Focus on $Mp^{dp} \bmod p$ calculation ($Mq^{dq} \bmod q$ similar)

```
For each bit i of secret dp
   perform "Square"
   if (bit i == 1)
     perform "Multiply"
   endif
endfor
```

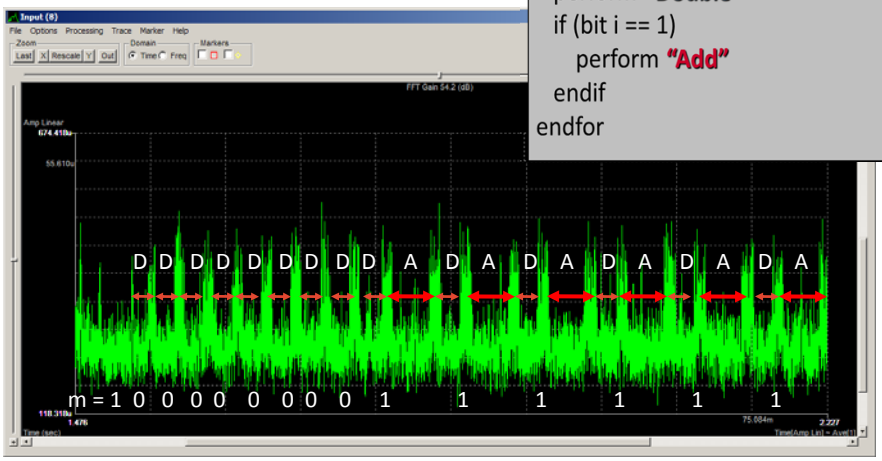


App Security Demo 2
Simple EM attack on ECC from 10 feet away

- ECC (Elliptic Curve Cryptography) App on PDA
  - Point multiplication (m * Q) over P-571 using open source crypto library
- Double-and-add algorithm to compute m*Q
- In ECC, double and add are very different operations
- The double/add execution sequence yields m !

```
For each bit i of secret m
  perform "Double"
  if (bit i == 1)
    perform "Add"
  endif
endfor
```

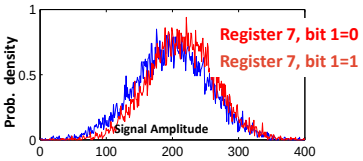

ECC Signal: Extracting Secret M



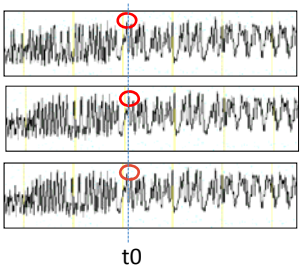

```
For each bit i of secret m
  perform "Double"
  if (bit i == 1)
    perform "Add"
  endif
endfor
```

DPA: Statistical techniques for analyzing data with low signal/noise ratios

- Signal / noise ratio may be very small
  - However, statistical influence remains…



Power signal amplitude at time t0



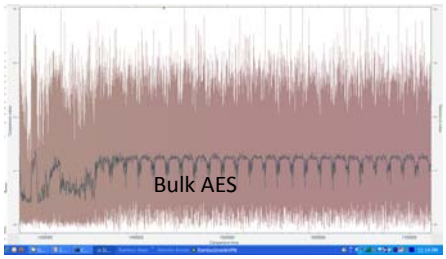
  - Eg. At time t0, mean of signals where register 7 bit 1= 0 is different from mean of signals where register 7 bit 0 = 0

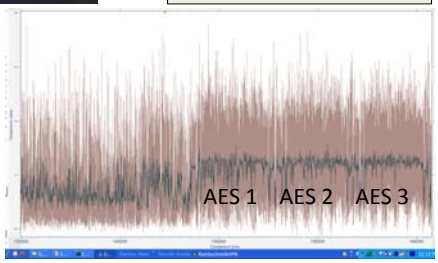
- DPA: Using statistical methods to analyze minute differences in power measurements due to the data being manipulated
- Similar analysis applies to EM measurements

Bulk AES Example

- Bulk AES encryption on another Android phone
  - App invokes the Bouncy Castle AES provider
  - Baseband m-field trace capture on a sampling scope

- Baseband
- Acq LPF = 100 MHz
- Filt BW = 60 MHz



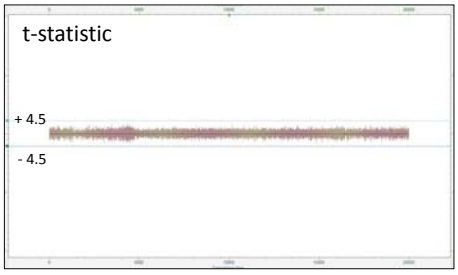


Efficient Leakage Testing

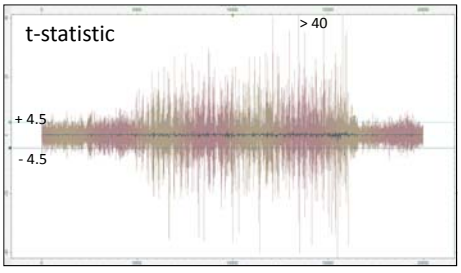
- Testing for all DPA leakage possibilities can be very a labor intensive, time consuming process
- Fortunately, we can test for leakage without actually doing full DPA key recovery
- Developed standardized test: Statistical analysis of operations to reveal presence of leakage

Bulk AES: Information leakage assessment

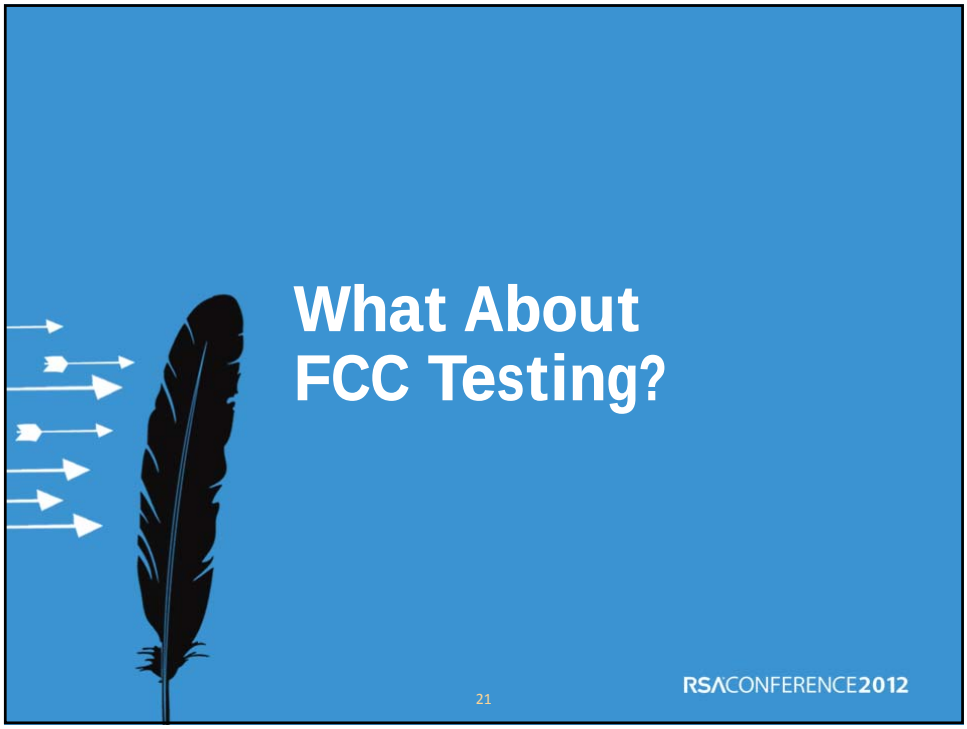
- Results of standardized leakage test (t-test)
  - Substantial DPA leakages are present



Control Group: t-test comparing average signal from Set 1 (random AES) with average signal from Set 2 (random AES)



Test Group: t-test comparing average signal from Set 1 (random AES) with average signal from Set 3(fixed AES)



FCC Part 15 Overview

- Covers nearly every electronics device sold in the US (similar regulations for other markets worldwide)
- Devices must be either verified or certified to *not cause harmful interference*
- Intentional transmitters go through a more complex process to receive device "Certification"
- Unintentional radiators get a "Declaration of Conformity" through a simpler process of verification
- Most mobile devices contain wireless links, and therefore need more difficult to obtain "Certification"

FCC Example with Numbers

- FCC part 15.109 (a) …the field strength of radiated emissions from unintentional radiators at a distance of 3 meters shall not exceed the following values:

  …

  Above 960 MHz: 500 microvolts/meter

- Received Power (dBm) =

Field Strength (dBuV/m)	[54.0	]
- 20 log Frequency (MHz)	[- 60.0	]
+ Antenna Gain (dBi)	[+10.0	]
- 77.2	[- 77.2	]

= -73.2 dBm Well above noise floor!

Does FCC Certification Prevent Radiating Secrets?

- No!
- Note all demonstrations use unmodified devices which are commercially sold – presumed FCC Certified
- Even GSM buzz doesn't meet FCC definition of harmful interference

DPA Countermeasures

- SPA/DPA immunity is possible and practical
  - But very different from a simple “bug fix”
- Security can involve a mix of countermeasures
  - At hardware, software and protocol layers
  - CRI invented the fundamental solutions to DPA, licenses patents, and assists licensees implement countermeasures in products
- Countermeasure overheads depends on
  - Algorithms being protected, leakage characteristics of the device, desired level of immunity, engineering constraints and design flexibility
  - Performance overhead can range from ~10% (e.g., RSA w/out CRT), ~25% (AES protocol countermeasures) to >400% (general purpose AES, other symmetric)

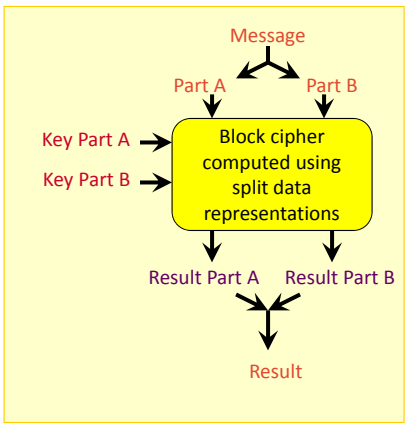
SPA / DPA Countermeasures

- SPA/DPA countermeasures: fundamental categories
  - Obfuscation
  - Leak Reduction
  - Balanced HW / SW
  - Amplitude & Temporal Noise
  - Incorporating Randomness
  - Protocol Level CM
- Cryptography Research has patented the fundamental solutions to DPA

A license is required to make, use, sell or issue DPA-resistant devices

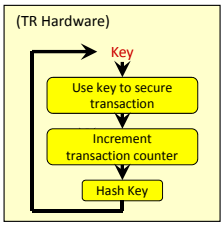
Example of a SW-Friendly Countermeasure: Masking

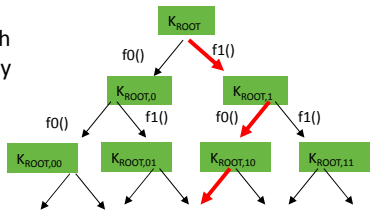
- Block ciphers can be implemented in ways that use random information to
  - Split key into two (or more) randomized parts
  - Split message into two (or more) randomized parts
  - E.g., Key = Key Part A ⊕ Key Part B
- Compute the block cipher using the two randomized, unpredictable parts
  - Correct answer is obtained, but no internal variable is correlated to the input and key



Protocol Level Countermeasures

- Problem: Protocols may allow attacker unlimited traces with a fixed key
  - O(2^{40}) traces: 10^{-10} bits leaking/transaction is too much
- Solution: Build protocols that survive information leakage
  - Design crypto with realistic assumptions about the hardware
  - Hardware has to be fairly good, but assumed to leak
  - Can obtain provable security against DPA with reasonable assumptions and significant safety margin
- Examples: symmetric key transactions, challenge response, authenticated encryption/decryption





CRYPTOGRAPHY RESEARCH a division of Rambus

RSACONFERENCE2012

Conclusions / Application Actions

RSACONFERENCE2012

Summary

- Electronic devices radiate information
- Shielding may not be sufficient nor appropriate for mobile devices with wireless capabilities
- Some platforms have effective HW & OS-level countermeasures
- On other platforms, users need to mitigate using software and protocol countermeasures
- Testing must be part of any security design

Apply Slide

- Application developers should understand how side channel information leaks affect critical applications.
- If no HW or OS-level platform countermeasures, examine the use of application and protocol countermeasures

Contact Information

Benjamin Jun (ben@cryptography.com)
Gary Kenworthy (gary.kenworthy@cryptography.com)

Cryptography Research, Inc.
www.cryptography.com

CRYPTOGRAPHY™ RESEARCH
a division of Rambus