MILCOM 2016
SECURE COMMUNICATIONS AT THE SPEED OF CYBER

Information Leakage Background and Threat Modeling

Suresh C. Kothari
Richardson Professor
Department of Electrical and Computer Engineering

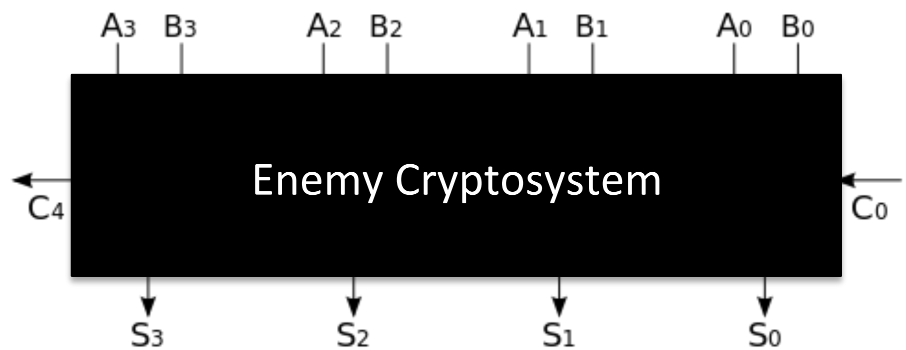
Ben Holland, Iowa State University

Acknowledgement: Team members at Iowa State University and EnSoft, DARPA contracts FA8750-12-2-0126 & FA8750-15-2-0080

BALTIMORE, MD • NOVEMBER 1–3, 2016

Side Channels

- Historically “side channels” were used to describe attacks to physical crypto hardware systems
  - Power analysis
  - Timing information
  - Acoustics
  - Faults
  - Electromagnetic radiation
    - Light, heat, IR, etc.
  - Not brute force/cryptanalysis
- Some operations require more time, power, etc. to complete than others

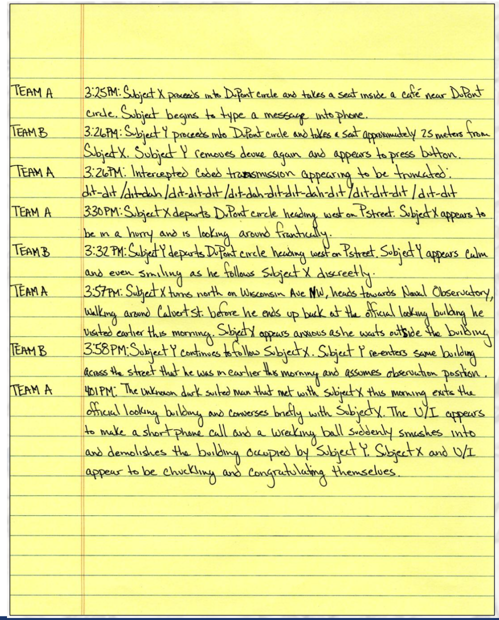


A_0	B_0	A_1	B_1	A_2	B_2	A_3	B_3	C_0
0	1	1	1	1	0	0	0	0
-	-	-	-	S_0	S_1	S_2	S_3	C_4
				1	0	0	1	0

1 0
1 1 0
+ 0 1 1
(1) 0 0 1

DARPA's Paper Shredder Challenge

- $50,000 prize to unscramble 5 shredded documents
- Puzzles were completely solved on December 2011 by team "All Your Shreds Are Belong To U.S."



TEAM A 3:25PM: Subject X proceeds into DuPont circle and takes a seat inside a café near DuPont circle. Subject begins to type a message into phone.

TEAM B 3:26PM: Subject Y proceeds into DuPont circle and takes a seat approximately 25 meters from Subject X. Subject Y removes device again and appears to press button.

TEAM A 3:26PM: Intercepted coded transmission appearing to be truncated: dit-dit /dit-dah /dit-dit-dit /dit-dah-dit-dit-dah-dit /dit-dit-dit /dit-dit

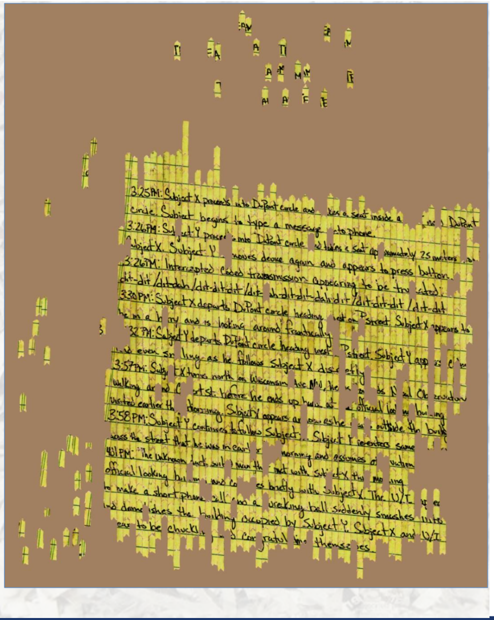
TEAM A 3:30PM: Subject X departs DuPont circle heading west on P street. Subject X appears to be in a hurry and is looking around frantically.

TEAM B 3:32 PM: Subject Y departs DuPont circle heading west on P street. Subject Y appears calm and even smiling as he follows Subject X discreetly.

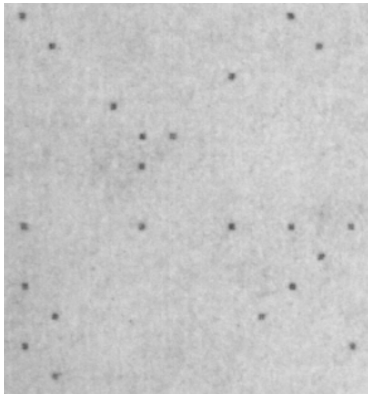
TEAM A 3:57PM: Subject X turns north on Wisconsin Ave NW, heads towards Naval Observatory, walking around Calvert St. before he ends up back at the official looking building he visited earlier this morning. Subject X appears anxious as he waits outside the building

TEAM B 3:58PM: Subject Y continues to follow Subject X. Subject Y re-enters same building across the street that he was in earlier this morning and assumes observation position.

TEAM A 4:01PM: The unknown dark suited man that met with Subject X this morning exits the official looking building and converses briefly with Subject X. The U/I appears to make a short phone call and a wrecking ball suddenly smashes into and demolishes the building occupied by Subject Y. Subject X and U/I appear to be chuckling and congratulating themselves.



- A little of life's irony…
  - ~9000 teams competed, 1 team solved all 5 puzzles
  - Solution used hidden printer dots added by printer manufacturers and U.S. Secret Service



  - Vision recognition software detected dots printed on paper and used dots as a reference guide to identify document fragments
  - Pro-tip: Burn your documents you really want gone…

Das Blinkenlights

ACHTUNG!

Alles turisten und non-teknischen looken peepers! Das computermaschine ist nicht füer gefingerpoken und mittengraben! Ist easy schnappen der springenwerk, blowenfusen und poppencorken mit spitzensparken.

Ist nicht füer gewerken bei dummkopfen. Das rubbernecken sightseeren keepen das cotton-picken hans in das pockets muss; Zo relaxen und watschen der blinkenlichten.

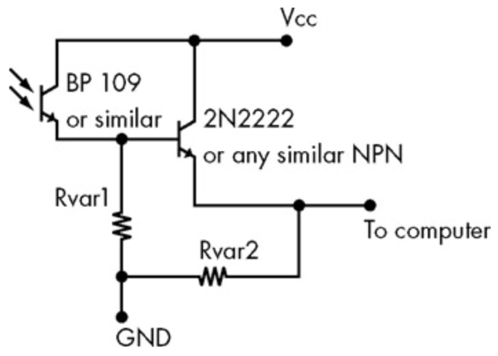
Das Blinkenlight

Historically, the blinking lights indicated important things like the state of the system, but as computers became faster and more reliable the lights were either removed or left as diagnostic indicators (example: networking hardware).

Blinkenlights Problem

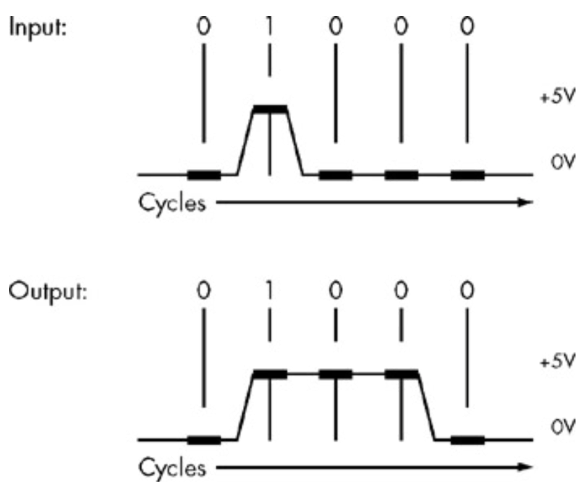
- LEDs on/off time is very fast (almost instant)
  - LEDs are usually used to control fiber optics
- LEDs were wired directly into the serial data line
  - Each blink is a 1 on your network, LED off is a 0
  - Too fast for a human eye
  - Not too fast for a circuit…and a telephoto lens!

Paper: Joe Loughry and David A. Umphress. 2002. *Information leakage from optical emanations.* ACM Trans. Inf. Syst. Secur. 5, 3 (August 2002), 262-289.



Blinkenlights Solutions

- Duct tape over the LEDs works, but we still want our blinkenlights!
  - Pulse Stretching ☹



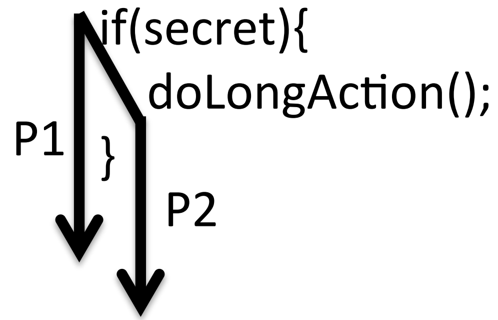
Still possible to recover 99.999988% of bits.
Error correction codes can help us guess the rest.

  - Better approach → Low frequency sampling with a latch till the next sample

Side Channel Origins

- Short story: optimizations
  - Reducing cost: power, heat, etc.
  - Increasing speed/efficiency
- Consider synchronous vs. asynchronous digital logic circuits
  - Synchronous circuits operate on a fixed clock, all operations take the same time, so the best case and worst case times are the same
    - Every case is the worst case
  - Asynchronous circuits operate without a clock independent of other modules, so there are distinct best, worst, and average cases.
    - Average case costs less than the worst case

Differential Branching



Path 1 Cost: Short
Path 2 Cost: Long

Toy Example

How many interactions with the *entrypoint* does it take to learn the *CONFIDENTIAL* value?

```java
public class SideChannelExample {
        private static final int CONFIDENTIAL = 666;
        public static boolean entrypoint(int param){
                int condition = CONFIDENTIAL & param;
                if(condition == 0){
                        for(int i=0; i<5; i++){
                                doSomethingExpensive();
                        }
                }else{
                        doSomethingCheap();
                }
                return CONFIDENTIAL == param;
        }
        private static void doSomethingCheap(){}
        private static void doSomethingExpensive(){
                for(int i=0; i<10000; i++){}
        }
}
```

Software Side Channels

- Software information leakage primarily through…
  - Timing information
  - Memory space usage
    - Content, order, size

Space/Time usage are related problems

- Optimizations create asymmetries everywhere…
  - Software algorithms
    - Branching, short-circuiting logic, looping, etc.
  - Compiler optimizations
  - Cache hits
  - Process scheduling
  - Branch prediction…and so on…

Demasking Google Users

1. Select Google users to target
2. Create a Google drive document and invite targets (uncheck option to send notification)
3. Using HTML/JavaScript create a spear-phishing site that identifies and customizes itself for the target
   - takes longer to call onerror if visitor is a target
   - Google has declined to fix this issue

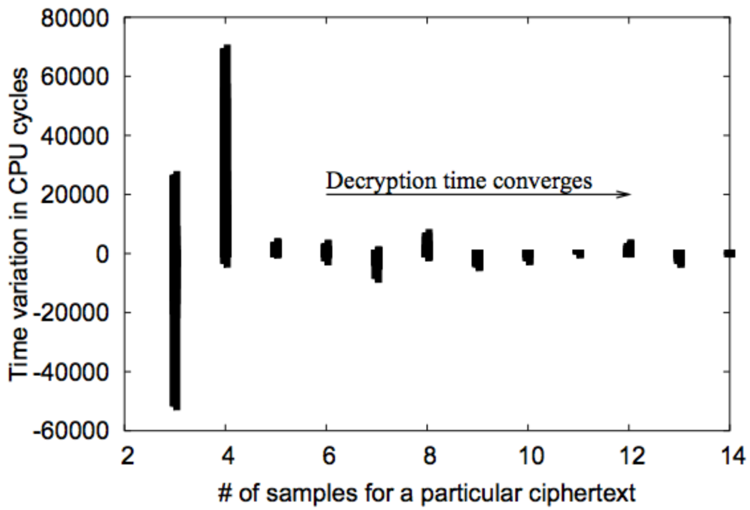
OpenSSL Vulnerability

- Timing attack against OpenSSL server to recover SSL private RSA key
  - RSA decryption: $m = c^*d \bmod N$, where $N = pq$
  - If you know the factorization of N, then $d = e^{-1} \bmod (p-1)(q-1)$
- Issue: Algorithm processing time was dependent on ciphertext and private key
  - Extra reductions in a Montgomery reduction (fast mod operation) when ciphertext (c) approaches a multiple of q ($c < q$ should be slower than decryption of $c > q$)
  - OpenSSL uses two different multiplication routines: when $c < q$ fast Karatsuba multiplication is used, otherwise the slower normal multiplication is used since $c > q$ is likely smaller when computing $c \bmod q$
- Performed over a network (dealing with network delays)

OpenSSL Vulnerability

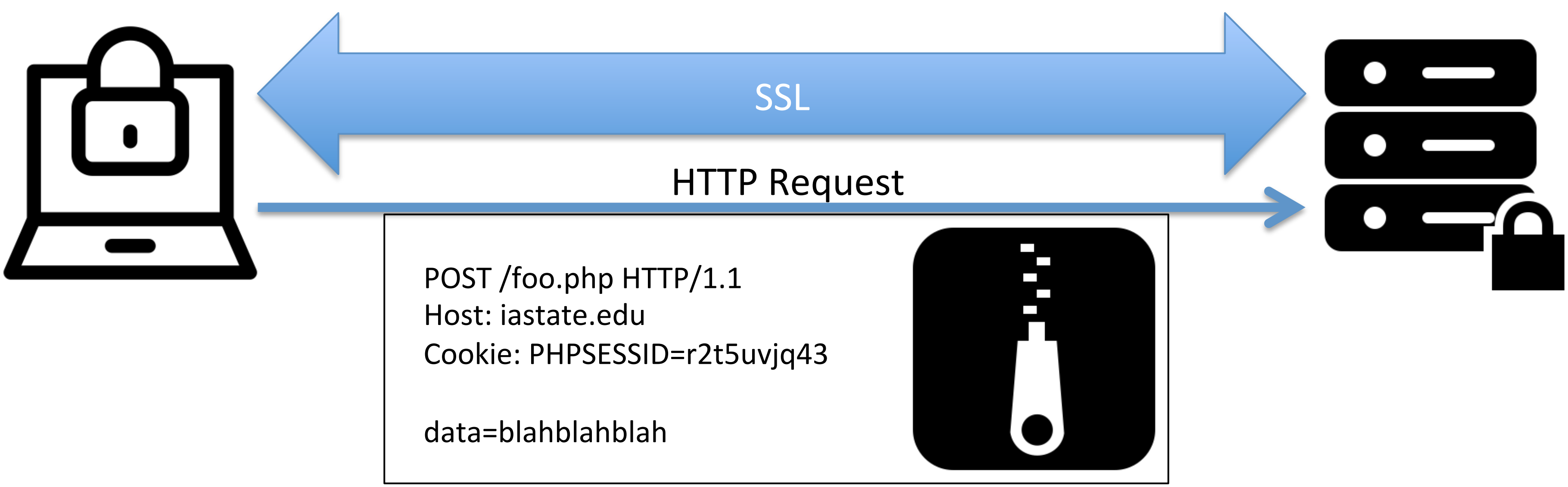
- Use of repeated requests to recover modulus *N* of the public key
  - Binary search of most significant bits
  - After half the bits are recovered factorization is completed with Coppersmith's algorithm

Note that not all of the secret was leaked! Just enough of the secret was leaked to make brute force search feasible.



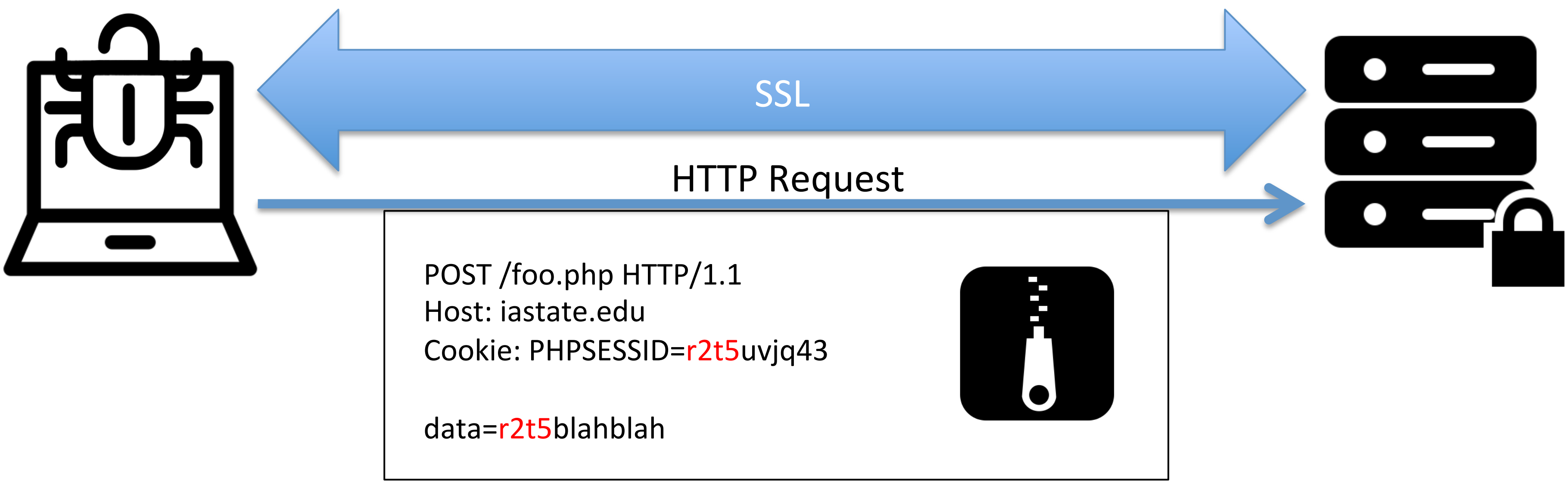
CRIME Vulnerability

- CRIME (Compression Ratio Info-leak Made Easy)
  - Chosen plaintext attack to create observable information leakage through compression ratios in order to recover an encrypted HTTP Cookie value
  - Requires ~6 requests per byte of the cookie value
  - 42% of web servers support TLS compression



CRIME Vulnerability

- CRIME (Compression Ratio Info-leak Made Easy)
  - Chosen plaintext attack to create observable information leakage through compression ratios in order to recover an encrypted HTTP Cookie value
  - Requires ~6 requests per byte of the cookie value
  - 42% of web servers support TLS compression



Underhanded C Contest

- Good example of a malicious side channel
  - Source has to be capable of passing a peer review
  - Execution has to appear to perform the task correctly
  - Challenge: Censor regions on a JPEG image, but somehow leak the redacted information
- Snippet of winning solution:

```
//read the ppm header
unsigned width,height,maxdepth;
fscanf(ppm,"P3\n%u %u\n%u\n", &width, &height, &maxdepth);
printf("P3\n%u %u\n%u\n", width, height, maxdepth);
```

  - Writes the magnitude of the red, green, and blue component for each pixel in order

Underhanded C Contest

- When we censor with a black rectangle we write 0's for the RGB pixel (a black pixel)
- PPM file format is flexible and implementation leaks how many digits each value originally when it processes the file character by character

	234 2 0 83 255 255 2 43 255
Implementation:	000 0 0 00 000 000 0 00 000
Should write:	0 0 0 0 0 0 0 0 0

- Perfect reconstruction for black/white images, otherwise partial reconstruction of blacked out region

Threat Modeling

- Budget in terms of active/passive operations?
- Threshold for # interactions?
- What are the observables?

A Segmented Side Channel Example

- Password characters can be extracted one at a time
  - Is there an upper bound on the number of extractable characters? What if we removed the randomness?

```
boolean authenticate(String input, String password) {
        for(int i=0; i<password.length() && i < input.length(); i++){
                if(input.charAt(i) == password.charAt(i)){
                        sleep(1000); // sleep 1 second
                        sleep(new Random().nextInt(10)); // sleep 0 to 10 ms
                } else {
                        return false;
                }
        }
        return true;
}
```

Thoughts on Noise

- Side channel signal degradation
  - Many sources of noise!
  - Requires additional statistical samples
  - Diminishing returns and increasing sample requirements eventually exceed brute force
- What is the *strength* of the side channel?

References

[1] DARPA Paper Shredder Challenge – http://archive.darpa.mil/shredderchallenge

[2] U.S. Secret Service Printer Program – http://seeingyellow.com

[3] Blinkenlights (Chapter 5) – Michal Zalewski. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. No Starch Press, San Francisco, CA, USA. Michal Zalewski. 2005.

[4] Demasking Google Users with a timing attack. Andrew Cantino. 2014.

[5] OpenSSL Timing Attack – Brumley, David, and Dan Boneh. Remote timing attacks are practical. Computer Networks 48.5 (2005): 701-716.

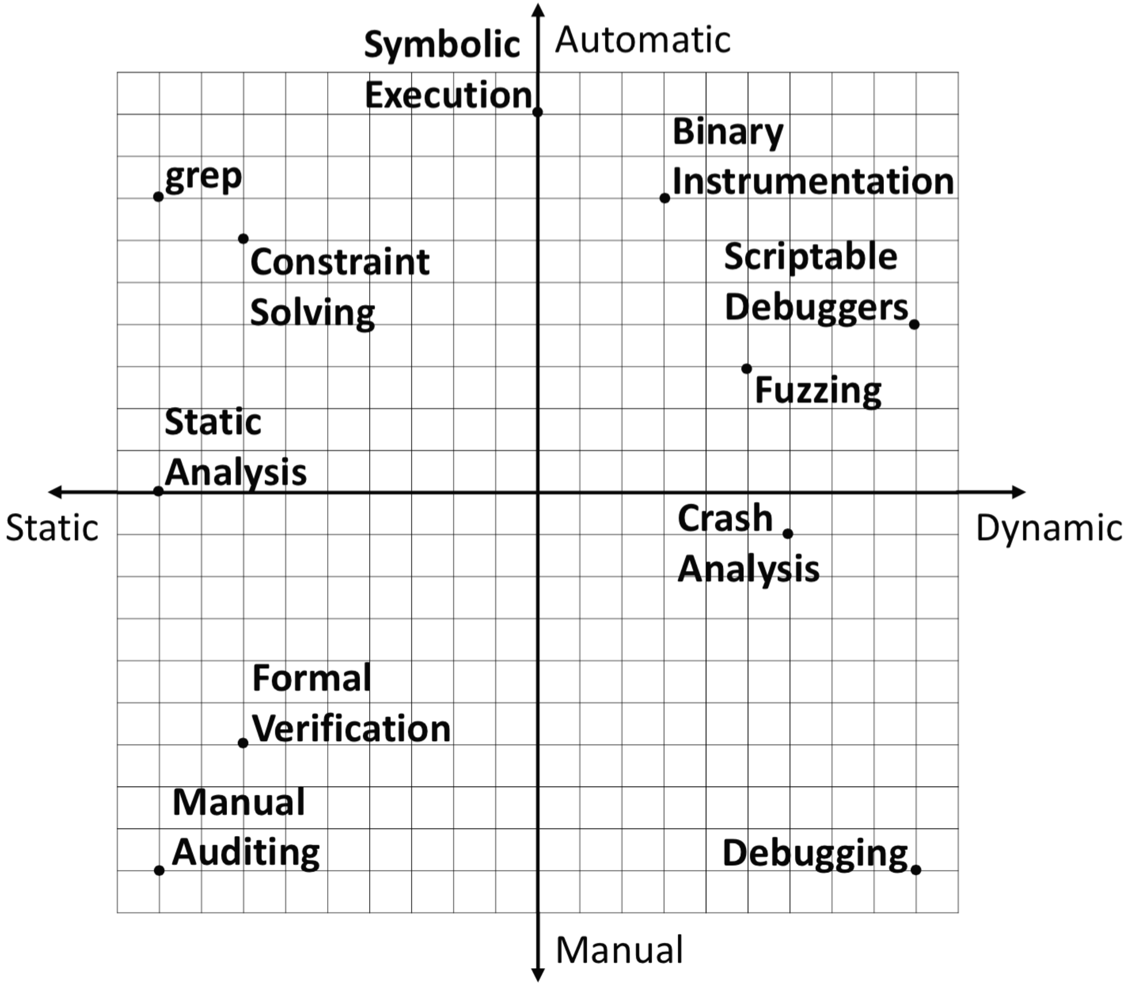
[6] Underhanded C Contest – http://notanumber.net/...the-leaky-redaction

[7] Eliminating Timing Side-Channels. A Tutorial. Peter Schawabe. ShmooCon 2015.

[8] Remote timing attacks are practical. Brumley, David, and Dan Boneh. Computer Networks 48.5 (2005): 701-716.

[9] Side Channel Attacks. John Franco. University of Cincinnati Network Security course lecture.

Sneak Peek



Source: Contemporary Automatic Program Analysis, Julian Cohen, Blackhat 2014