# Blind Return Oriented Programming (BROP)

When hacking software, there are three exploit scenarios:

1. Open-source (e.g., Apache)
2. Open-binary (e.g., Internet Explorer)
3. Closed-binary and source (e.g., some proprietary network service)

This work studies whether it is possible to attack the third case.

The BROP attack makes it possible to write exploits without possessing the target's binary. It requires a stack overflow and a service that restarts after a crash. Based on whether a service crashes or not (i.e., connection closes or stays open), the BROP attack is able to construct a full remote exploit that leads to a shell. The BROP attack remotely leaks enough gadgets to perform the write system call, after which the binary is transferred from memory to the attacker's socket. Following that, a standard ROP attack can be carried out. Apart from attacking proprietary services, BROP is very useful in targeting open-source software for which the particular binary used is not public (e.g., installed from source setups, Gentoo boxes, etc.).

The attack completes within 4,000 requests (within minutes) when tested against a toy proprietary service, and real vulnerabilities in nginx and MySQL.

The fundamental problem sometimes seen in servers is that they fork a new worker process after a crash, without any rerandomization (e.g., no execve follows the fork). nginx for example does this.

The paper describing the work is:

- A. Bittau, A. Belay, A. Mashtizadeh, D. Mazières, D. Boneh: Hacking Blind. In *Oakland* 2014. [slides]

# Attack outline

1. Break ASLR by "stack reading" a return address (and canaries).
2. Find a "stop gadget" which halts ROP chains so that other gadgets can be found.
3. Find the BROP gadget which lets you control the first two arguments of calls.
4. Find a call to strcmp, which as a side effect sets the third argument to calls (e.g., write length) to a value greater than zero.
5. Find a call to write.
6. Write the binary from memory to the socket.

7. Dump the symbol table from the downloaded binary to find calls to dup2, execve, and build shellcode.

# Downloads

Braille

A fully automated tool that conducts a BROP attack (from crash to remote shell) when supplied with an input string that crashes a server due to a stack overflow.

Optimized nginx BROP exploit

A generic 64-bit exploit for nginx 1.4.0 that uses BROP, optimized for nginx's case. This also includes an IP fragmentation router to make the attack possible on WANs. nginx does a non-blocking read on a 4096 byte buffer, and typical MTUs are 1500, so IP fragmentation is needed to deliver a large TCP segment that will result in a single read of over 4096 bytes.

Ali's server

The toy proprietary service written by a colleague used as a test case in the paper for hacking without neither binary nor source code knowledge.