

Detecting and Preventing Attacks with Vulnerability Signatures



Nikita Borisov (PI), David Nicol and William Sanders (co-Pis), UIUC

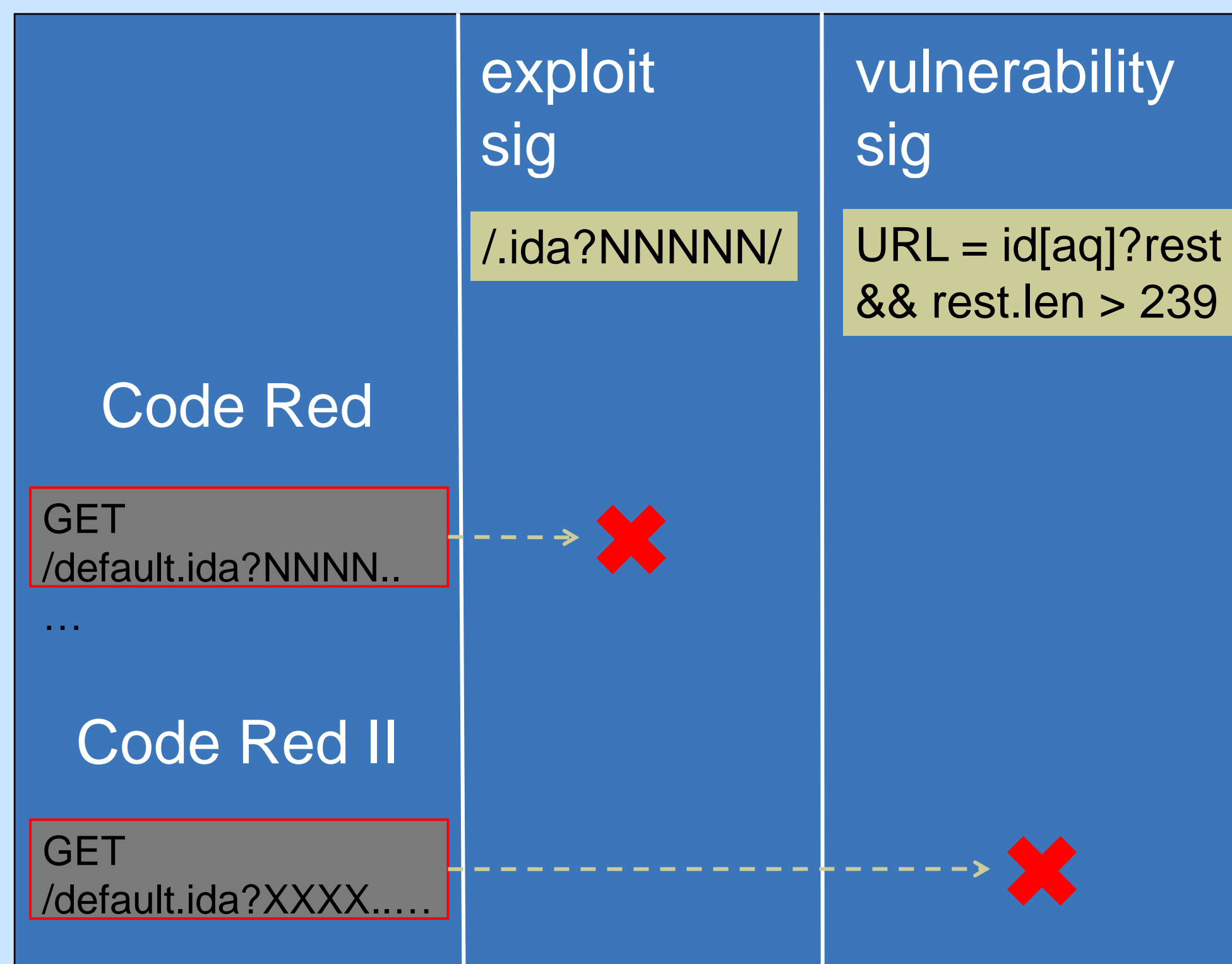
<http://hatswitch.org/research/vulnsigs/>

Vulnerability Signatures at Line Speed

Vulnerability signatures use detailed protocol knowledge to precisely describe how a network message leads to an exploit. However, generic protocol parsers used for this purpose are too heavy-weight.

Modern IDS systems are already struggling with Gbps+ of network traffic. By specializing the parsing for the specific goal of vulnerability signatures, and by using fast hardware primitives, we can achieve line speed performance

Our research aims to make vulnerability signatures practical for Networked IDS



Approach and Impact

New approach

- Fast pattern matching primitives
- Specialized parsing
- Hardware acceleration

Research Impact

- Improved performance of vulnerability signatures
- VS filtering practical at border firewalls

Based on a vulnerability study, the full complexity of protocol parsing is not necessary for vulnerability signatures. Instead, we can deploy fast pattern-matching primitives, paired with control logic handlers, and drastically improve matching speed.

Status:

Text Protocols — built a compiler that generates code, using S/W pattern matchers

Binary Protocols — build hand-coded parser instances, working on compiler now

