What makes software exploitation hard?
Project Zero mission:

Make 0day hard.
$130,000
Project Zero approach:

- Vulnerability research
- Exploit mitigations
Project Zero results:

- 600 vulnerabilities
- 40 technical blog posts
- 5+ shipped exploit mitigations
An observation on the adversarial nature of things:

1. Defense aims to understand attack.
2. Attack aims to limit or disrupt defense's data.
3. Defense *must* model attack.
In the mind of a hard working attack researcher....

- "Will I be able to find a good vulnerability?"
- "What are the chances this bug will get fixed?"
- "How long will it take to write an exploit?"
- "How can I make this exploit reliable?"
Vulnerability Research Strategy

Eliminate Low-hanging Fruit

- Utilize machine resources
- Bring an end to dumb-fuzzing
- Incrementally improve fuzzing state-of-the-art

Last Step of the Bug Chain

- Find surfaces with high contention
- e.g. kernel, sandbox
- Use all means possible to find+fix bugs
Target Selection

● Balance of:
  ○ Observed attacks
  ○ External feedback
  ○ Internal deduction

● Today, we focus heavily on endpoint attacks
  ○ Mobile: Android, iOS
  ○ Desktop: Windows, OSX, Linux
  ○ Browsers: Chrome, Internet Explorer, Firefox
  ○ Documents: .doc, .pdf
  ○ Endpoint security: AV
Exploit Mitigation Strategy

Review
- Document newly implemented mitigations
- Verify correctness
- Discover edge cases

Design
- Perform exploit development
- Find fragility points
- Share ideas for new mitigation designs
Mitigation Taxonomy

- **Type 0 - Strong Mitigation**
  
  *End a bug class.*

- **Type 1 - Weak Mitigation**
  
  *End an exploitation technique.*

- **Type 2 - Attack Surface Reduction**
  
  *Remove a set of exposed functionality.*

- **Type 3 - Chain Extension**
  
  *Increase the number of bugs required in an exploit.*
Case Study: Adobe Flash

- 180 vulnerabilities reported - fuzzing and manual review
- Heap partitioning and ASLR improvements
- Observed price increase: ~60%
What makes exploitation hard?
What makes exploitation hard?

- Advance the state of the art in vulnerability research and exploit mitigation.
What makes exploitation hard?

- Advance the state of the art in vulnerability research and exploit mitigation.
- Exploits are chains.
What makes exploitation hard?

● Advance the state of the art in vulnerability research and exploit mitigation.

● Exploits are chains.
  ○ Make each link harder to forge.
  ○ Lengthen the chain.
Thank you!

Project Zero Blog: https://googleprojectzero.blogspot.com/

Project Zero Issue Tracker (Fixed Bugs): https://code.google.com/p/google-security-research/issues/list?can=1&q=status%3AFixed