MEDICAL DEVICE SECURITY

Chris Clark – Senior Security Engineer

June 5, 1015
Who am I?

Chris Clark
Senior Security Engineer
Codenomicon
DISCLAIMER: Before we start...

This is **not** about...

- Closed vs open source
- Any particular company
- A particular vertical

The behavior we are about to discuss is found across multiple verticals.
Why not?
Next level
Total Vulnerability Management

Known Vulnerability Management
- Compliance, policy, and patch management
- Threat intelligence, known vulnerability scanning

Unknown Vulnerability Management
- Whitebox Approach: Source code analysis and source code scanning
- Blackbox Approach: Fuzzing, binary analysis other dynamic methods

© 2015 All Rights Reserved
What is next? FUZZING
NORMAL HTTP PROTOCOL DATA EXCHANGE ...

GET/HTTP/1.1
Host: www.codenomicon.com:80
Connection: Keep-Alive
User-Agent: Codenomicon-Defensics
Accept: text/html,image/jpg
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 Ok
Server: Secure-Master5000.v2.0
Location: www.codenomicon.com
Content-Type: text/html
Content-Length: 1337
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>

info@codenomicon.com
FUZZING:
SEND MALFORMED DATA TO AN INTERFACE & MONITOR BEHAVIOR ...

GET aaaaaaaaaaaaaaaaaa HTTP/1.1
Host: www.codenomicon.com:80
Connection: Keep-Alive
User-Agent: Codenomicon-Defensics
Accept: text/html,image/jpeg
Accept-Language: en-US,en;q=0.9

HTTP/1.1 404 Page Not Found
Server: Secure-Master5000.v2.0
Location: www.codenomicon.com
Content-Type: text/html
Content-Length: 0
Connection: close

info@codenomicon.com
FUZZING: ANOMALIES IN ONLY ONE FIELD

SEND MALFORMED DATA TO AN INTERFACE & MONITOR BEHAVIOR ...

GET HTTP/1.1
Host: www.codenomicon.com:80
Connection: Keep-Alive
User-Agent: Codenomicon-Defensics
Accept: text/html,image/jpeg
Accept-Language: en-US,en;q=0.9

HTTP/1.0 412 precondition failed

info@codenomicon.com
FUZZING: ANOMALIES IN MULTIPLE FIELDS
SEND MALFORMED DATA TO AN INTERFACE & MONITOR BEHAVIOR ...

GET/HTTP/1.1
Host: www.codenomicon.com:80
Connection: Keep-Alive
User-Agent: Master5000.v2.0
Accept: text/html,image/jpeg
Accept-Language: en-US,en;q=0.9

HTTP/1.1 404 Page not found
Server: Secure-Crash5000.v2.0
Location: www.codenomicon.com
Content-Type: text/html
Content-Length: 1337
Connection: close

<html>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 2.0//EN">
<html>
FUZZING: ANOMALIES CAN CAUSE A SYSTEM FAULT
SEND MALFORMED DATA TO AN INTERFACE & MONITOR BEHAVIOR ...

GET [????:0] HTTP/1.1
Host: www.codenomicon.com:80
Connection: Keep-Alive
User-Agent: Codenomicon-Defensics
Accept: text/html,image/jpeg
Accept-Language: en-US,en;q=0.9

Failed to parse request
Segmentation Fault
core dumped

# # #

info@codenomicon.com
Demonstration 1

• Bluetooth
• Low level weakness
• Out of site, out of mind
• Still your problem
Conclusion

• Medical device security requires a multi pronged approach

• Devices are not the only source of vulnerabilities, check the “glue”

• Know what you have purchased. Use a BOM...

• Fuzz everything

• Test, Test, Test
Chris Clark
chris@codenomicon.com