

# Building a Trustworthy Computing Platform

Gabriel L. Somlo, Ph.D.  
<glsomlo@cert.org>

SEI, CERT Division  
Carnegie Mellon University  
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

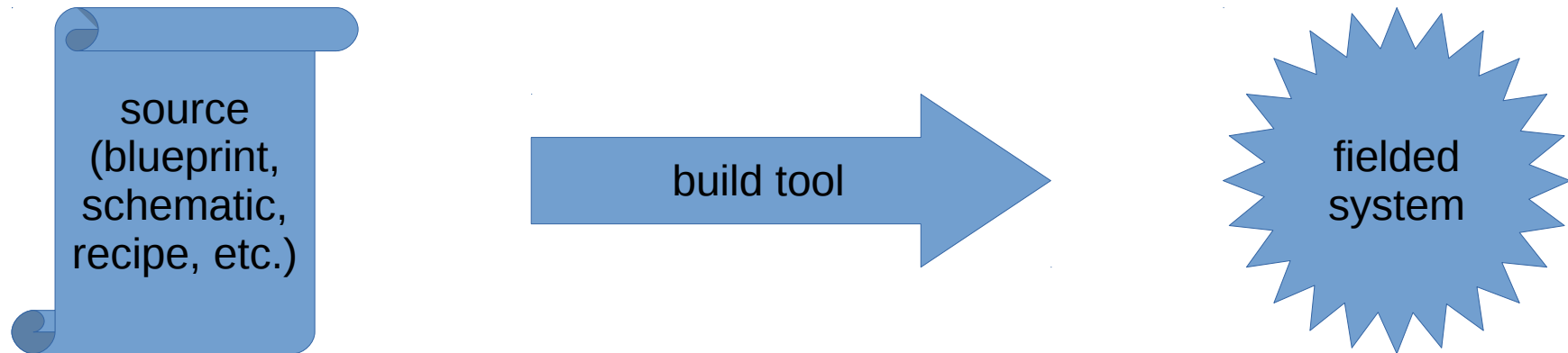
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

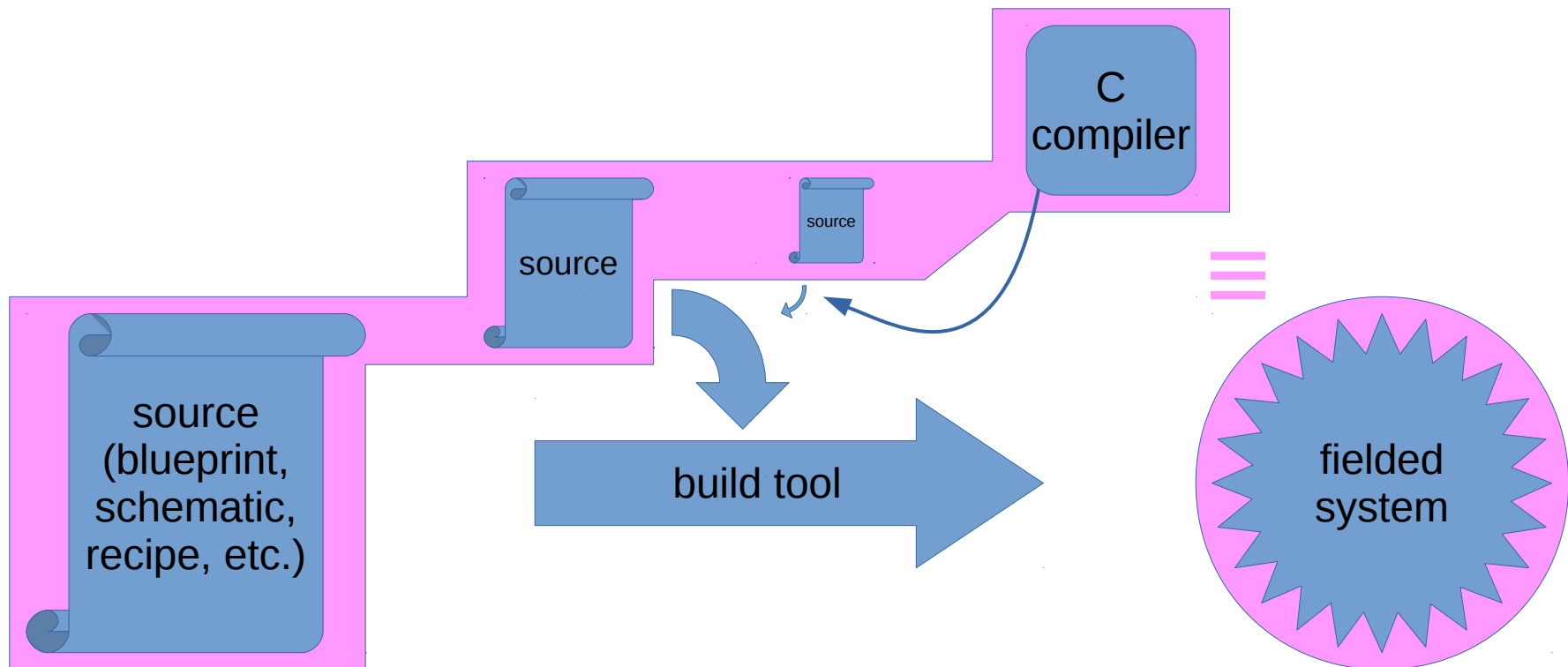
Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0566

# Trust Anchors for Fielded Systems



# Trust Anchors for Fielded Systems



# Trusting Trust: Problem and Solution

- **Self-propagating compiler hack** (Ken Thompson)
  - Malicious C compiler inserts Trojan during *victim program* build
    - Clean source → malicious binary
      - Including *compiler's own* sources!
    - Compiler source hack *no longer needed* after 1<sup>st</sup> iteration!
- David A. Wheeler's defense: **Diverse Double Compilation**
  - Suspect compiler A: source  $S_A$ , binary  $B_A$
  - Trusted compiler T: binary  $B_T$
  - $S_A \rightarrow B_A \rightarrow X$                        $S_A \rightarrow B_T \rightarrow Y$ 
    - X and Y are functionally identical, but different binaries
  - $S_A \rightarrow X \rightarrow X_1$                        $S_A \rightarrow Y \rightarrow Y_1$ 
    - $X_1$  and  $Y_1$  must be identical binaries (since X, Y functionally identical)

# Recommendations

- Retain ability to *field strip* our cyber-weapons!
  - Require capability to rebuild system from *sources*
    - *Including* tool chain sources: HDL & software compilers!
  - Show of *good faith* from upstream supplier(s)
  - Built-in sustainment capability from *day one*
    - Solve “Trusting Trust” concerns
      - Available source code (to everything) acting as trust anchor

# Bootstrapping a Trustworthy Platform

- Use DDC to obtain a clean C [cross-]compiler
- [Cross-]compile HDL compiler toolchain
- Cross-compile target OS (kernel, glibc, utilities)
- Build FPGA bitstream with HDL toolchain
- Boot target OS on FPGA
  - **Self-hosting** from this point forward
    - Any system component can be (re)built on the system itself!
  - Trust anchor: the cumulative set of source code
    - HDL, OS (kernel, glibc, utilities), and Compilers (C & HDL)

# List of Ingredients

- FPGA development board
  - Lattice ECP5 Versa: [LFE5UM5G-45F-VERSA](#)
- Free/Open HDL (Hardware Description Language) toolchain
  - Verilog front-end: <https://github.com/YosysHQ/yosys>
  - ECP5 device db. & bitstream tools: <https://github.com/SymbiFlow/prjtrellis>
  - Place & Route back-end: <https://github.com/YosysHQ/nextpnr>
- Free/Open 64-bit CPU (RISC-V ISA)
  - RocketChip: <https://github.com/freechipsproject/rocket-chip>
- Free/Open System-on-Chip (SoC) environment (sys. bus & peripherals)
  - LiteX: <https://github.com/enjoy-digital/litex>
- Software stack (Linux, GCC, glibc)
  - Fedora: <https://fedoraproject.org/wiki/Architectures/RISC-V>



# Simplified Computer Architecture

