SSSS’20 will be an online hands-on learning institute. Come learn about a completely new family of tools that offer a transformational approach to reducing risk and attack surface in cyber systems.

More Details and Registration at: [https://www.cerias.purdue.edu/site/ssss20](https://www.cerias.purdue.edu/site/ssss20)

Why Attend?

New cyber exploits keep coming and coming:
- Software is inherently insecure. Popular apps continue to yield new bugs for relatively small attacker resource investment.
- Patching is a never-ending battle. Most software defense strategies are reactive. Bugs cannot be fixed until they are found.

Explore new cyber tools to get ahead of the adversary:
- Proactively cut needless cyber attack surface that exists in your system. The amount of unnecessary risk may surprise you!
  - Learn to debloat legacy code
  - Learn to cut unnecessary features from deployed software
- Explore how this emerging pipeline of post-build security capabilities could harden your critical systems.

SSSS’20 is an opportunity to get hands-on experience with capabilities drawn from R&D efforts under ONR’s Total Platform Cyber Protection (TPCP) program. Attendees will also give feedback to help influence continued development.

**Tutorial Agenda**

**August 3:** Five exciting pre-tutorial demos on BIOS debloating, CPS fuzzing, binary rewriting, mobile forensics and OS hardening

**August 4:**
- **RAZOR** Post-deployment software debloating
- Binary debloating through control-flow trimming

**August 5:**
- **Less-is-More** debloating dynamic web apps
- **JDebloat** Java bytecode debloating and delayering

**August 6:**
- **Embrittle** Binary diversification and fault encouragement
- **CBAT** Binary patch verification

**August 7:**
- Automated capabilities restriction for Docker containers
- Protocol customization and fuzzing

Each three-hour tutorial consists of
(i) a short presentation;
(ii) a demo of tool features; and
(iii) hands-on exploration with the tool.