GRAND CHALLENGES FOR EMBEDDED SECURITY RESEARCH IN A CONNECTED WORLD

Computing Community Consortium (CCC) Visioning Workshop Report

Tomas Vagoun
Cybersecurity and Privacy R&D Technical Coordinator
National Coordination Office for Networking and Information Technology R&D

Presented on behalf of CCC

CCC
Computing Community Consortium
Catalyst

COMPUTING COMMUNITY CONSORTIUM

The **mission** of the Computing Research Association's Computing Community Consortium (CCC) is to **catalyze** the computing research community and **enable** the pursuit of innovative, high-impact research.

Bring the computing research community together to envision audacious research challenges.

Communicate these challenges and opportunities to the broader national community.

Facilitate investment in these research challenges **by key stakeholders**.

Inculcate values of **leadership** and service by the computing research community.

Inform and influence early career researchers to engage in these community-led research challenges.

CCC VISIONING PROCESS

- **Winter 2017:** Kevin Fu (CCC Council Member from 2015-2019) proposes a workshop to address the security challenges of embedded systems.
- **Spring 2018:** USENIX agrees to a CCC proposal to co-locate the embedded security workshop at the 27th USENIX Security Symposium (2018).

Workshop organizers:

Farinaz Koushanfar
UC San Diego

Kevin Fu
University of Michigan

Wayne Burleson
UMass Amherst

CCC VISIONING PROCESS

- **Spring/Summer 2018:** The CCC releases a call for white papers to identify workshop attendees.

- **August 2018:** A 1-day workshop is held in Baltimore, Maryland, co-located with USENIX Security 2018. Over 50 participants from academia, industry, and government agencies.

- **May 2020:** CCC releases a workshop report titled *Grand Challenges for Embedded Security Research in a Connected World* based on the workshop's discussions. Click link for report: https://cra.org/ccc/wp-content/uploads/sites/2/2020/05/CCC_Embedded_Security_Report_final.pdf

- **August 2020:** CCC Briefing on the Embedded Security workshop and report to NITRD CSIA IWG.

LEADERSHIP IN EMBEDDED SECURITY WORKSHOP

- The workshop focused on 5 main themes:
  - **Medical/wearable devices**
  - **Autonomous systems (drones, vehicles, robots)**
  - **Smart homes**
  - **Industry and supply chain**
  - **Critical infrastructure**
- Most of the workshop was spent in breakout groups built around each of the 5 themes.
- The workshop also included:
  - Opened with keynote address from Sam Fuller (CTO Emeritus of Analog Devices).
  - Presentation from Farinaz Koushanfar on ML and embedded security.
  - Two panels: one featuring international perspectives and one highlighting U.S. federal agency program managers.

WORKSHOP PARTICIPANT INSTITUTIONS

- University of Cambridge
- Dartmouth & University of Michigan
- Florida Atlantic University
- National Security Agency
- University of Massachusetts Amherst
- University of South Florida
- MIT Lincoln Laboratory
- ETH Zürich, Switzerland
- Adventium Lab
- Virginia Tech
- Georgia Tech
- University of Michigan
- University of Louisiana at Lafayette
- Food and Drug Administration
- University of Michigan
- CTO Emeritus of Analog Devices
- University of Pennsylvania
- Robert Bosch LLC
- University of Illinois
- University of Massachusetts Amherst
- Boston Scientific
- MIT Lincoln Laboratory
- University of Michigan
- Siemens Corporation
- Korea Advanced Institute of Science and Technology
- University of California, San Diego
- National Science Foundation
- George Washington University
- University of Pennsylvania
- University of Maryland
- University of Colorado Boulder
- Department of Homeland Security
- Department of Defense
- Duke University
- North Carolina State University
- Visa Research
- Howard University
- University of Michigan
- Virginia Tech
- Dartmouth College
- University of North Texas
- Cornell University
- NITRD
- KU Leuven – COSIC
- Purdue University
- Zhejiang University
- University of Adelaide

PROGRAM MANAGER PANEL

Tomas Vagoun
NITRD

Douglas Maughan
Department of Homeland Security

Sandip Kundu
National Science Foundation

Brian Fitzgerald
FDA

Key Challenges and Recommendations Identified During the Workshop

MEDICAL DEVICES & WEARABLES

Overview:

- Medical and health devices, both implanted and wearable are strictly regulated by the FDA for safety and effectiveness to balance the benefits to patient health against the risks from using any medical device.

- However, existing regulations for the safety and privacy (i.e., HIPAA) issues related to medical devices do not cover information security or cyberphysical attack situations.

- Furthermore, fitness and personal health monitoring devices present numerous vulnerabilities and are not currently regulated.

MEDICAL DEVICES & WEARABLES

Challenges:

- Long legacy tail makes it challenging to change or update system interfaces or add new procedures (such as authentication protocols).
- Severe power and energy constraints of wearable, mobile, and implantable medical devices.
- Software, for example cloud-based services, when seen as a medical device, intersects and sometimes conflicts with the existing regulatory structures such as HIPAA.
- Globalization and distribution of medical devices away from the countries of origin.

MEDICAL DEVICES & WEARABLES

Recommendations:

- The application of classic cryptography, security, and control theory (which can be used to model and study impact of various attacks on cyber-physical systems as well to mitigate damage) to the vulnerabilities and attack surfaces could yield novel solutions.

- Stronger authentication protocols for devices that leverage unique features related to the physics, locality, or possibly distance to/from device.

- Ongoing efforts to create devices and systems with appropriate failback solutions and safe-modes can enable innovative applications while also limiting the risks.

DRONES AND TRANSPORTATION

Overview:

- Our traditional modes of transportation, such as cars and airliners, are increasingly computerized, connected, and thus vulnerable to cyber-attacks.

- At the same time, these modes of transportation are more and more autonomous, from cars to public transportation to (potentially) flying taxis.

- Autonomy also enables the emergence of new, smaller logistical capabilities such as flying drones for package delivery.

DRONES AND TRANSPORTATION

Challenges:

- These transportation systems directly interact with the physical world, in many cases have real-time requirements, and have the capability to harm people.
- Transportation systems have long lifespans on the order of decades with multiple patching and testing cycles. Note that some (e.g. Tesla) are now pushing software updates however this is far from widespread. Software updates can also introduce vulnerabilities.
- Sensors in these systems are often easier to spoof than human eyes.
- How do you share and manage electronic keys and consumer data?

DRONES AND TRANSPORTATION

Recommendations:

- Develop a methodology and tools (including formal methods) that incorporate security from the conception of the vehicle and enable reasoning about multiple layers (control, software, hardware) with different assumptions.

- This methodology should also be able to leverage interactions among multiple layers or physical properties of existing systems to enhance the security of the overall vehicle.

SMART HOMES

Overview:

- Currently, embedded home systems operate technologies from simple light switches that can be turned on with a cell phone, to integrated home fire alarms, security alerts, and health monitoring systems (such as sensors that detect falls).

- These home systems operate in conjunction with third parties including smart electric power meters from the electricity service provider, or mobile systems that are found on private automobiles, which may share controls with the garage door opener.

- Such embedded technologies are less regulated and more likely to be operated by a non-professional.

SMART HOMES

Challenges:

- Operation of the system by non-professionals with little knowledge of security requires a robust system that does not rely on outside intervention for configuration.

- Current technologies are not always integrated though there is a growing emphasis on standardization. For instance, the fire alarm and door lock systems may be from different vendors and fail to communicate with one another.

- The richness of the system is also likely to create fresh types of side channels such as the ability to use fluctuations on the power system to detect, say, the program being watched on the home TV.

- The information collected from individuals in their homes has obvious privacy implications and users will expect a high level of security to protect their sensitive information.

SMART HOMES

Recommendations:

- It is necessary to develop some kind of rely-guarantee framework (a kind of concurrent software verification technique) in which components can announce their security properties along with the assumptions they expect from their environment.

- Answers to the following questions must be generated through regulations:
  - Who should patch or update devices to assure continued protection?
  - Should the lifetime of devices match those of home ownership? Or, should there be models of transfer of devices to the new owner?

INDUSTRY AND SUPPLY CHAIN

Overview:

- Embedded systems rely heavily on software and firmware, but even more so they rely on the hardware that executes the code and makes the system real.

- Due to the long lifetime of industrial and supply-chain systems, some of this hardware is so old that new parts are nearly impossible to come by and replacement parts must be purchased from third parties, with varying degrees of success and fidelity.

- Even when new systems are built, they are often beholden to legacy interfaces for the sake of interoperability.

INDUSTRY AND SUPPLY-CHAIN

Challenges:

- Old systems and protocols are challenging to secure retroactively.
- Old hardware is similarly challenging to secure, and also challenging to acquire securely. Due to their age, they are often highly resource constrained, leaving little headroom to accommodate updated software or firmware with modern cryptographic and defensive technologies.
- Designing a safe and secure modern Application-Specific Integrated Circuit (ASIC) is challenging and expensive, often costing up to 100 million dollars.[1]

1. DARPA, "Circuit Realization at Faster Timescales (CRAFT)" https://www.darpa.mil/program/circuit-realization-at-faster-timescales

INDUSTRY AND SUPPLY CHAIN

Recommendations:

- Retaining the capability to manufacture new parts is a key solution to the threat of counterfeits. Ideally, a vendor that is no longer interested in manufacturing a part — or worse, a vendor that goes out of business altogether — should be required to yield their design to others who may wish to do so.

- For newer designs, so-called “split ASIC” and multi-chiplet techniques can divide the design into separate pieces that can be sent to separate fabrication facilities, complicating an adversary’s efforts.

SMART GRID AND CRITICAL INFRASTRUCTURE

Overview:

- Electric meters once passively recorded the accumulated flow of current into a household or business and were read monthly. Smart meters now record and report power consumption on a second-by-second (or finer) basis in real time, permitting charging based on time of use.

- More recently, “smart grid” has broadened to incorporate grids in which the infrastructure includes a range of technologies that can more generally sense and control its own operation.

- These new abilities can be used to take advantage of distributed power generation based on renewable sources (solar panels, wind turbines), to provide earlier detection and location of outages, and to control power flow among regions more safely and efficiently.

SMART GRID AND CRITICAL INFRASTRUCTURE

Challenges:

- Traditional centralized power generation is becoming more distributed as smaller scale generation with decentralized ownership and control (often “behind the meter”) becomes more economical.

- More active management of power demand is likely to accompany this transition, but unexpected dependencies between infrastructures are likely to be revealed, particularly in emergency situations.

- Failures and attacks may propagate in unexpected ways and pricing will become more dynamic.

SMART GRID AND CRITICAL INFRASTRUCTURE

Recommendations:

- Educating power companies about the effects of their buying decisions is crucial, and appropriate application of cryptographic technologies can solve some problems in this domain.

- Cryptography can assure the integrity of control signals even if they pass through untrusted domains, for example.

Common and Distinguishing Themes

COMMON THEMES

Common Themes and Challenges to Embedded Security	Smart Homes	Medical	Transportation Systems & Autonomous Vehicles	Industrial Control	Supply Chain	Smart Grid & Infrastructure
Long Life Time	✓	✓	✓	✓	✓	✓
Need to Accommodate Legacy Systems	✓	✓	✓	✓	✓	✓
Classic Control Theory	✓	✓	✓	✓	✓	✓
Consumer Privacy	✓	✓	✓			✓
Increasing Autonomy			✓	✓		
Power & Energy Constraints		✓				✓
Authentication in Emergency Situations	✓	✓	✓	✓		✓
Globalization	✓	✓	✓		✓	
Diverse Users & User Skill Level	✓	✓	✓			
Software as the Service in the Cloud	✓	✓				
Cloud Increased Multi-Vendor Interoperation	✓	✓	✓			✓
Concentrated Intellectual Property				✓	✓	

Figure 1. Overlap of Common Themes and Challenges in Embedded Security by Application Area

COMMON THEMES

Potential Novel Solutions to Embedded Security Challenges	Smart Homes	Medical	Transportation Systems & Autonomous Vehicles	Industrial Control	Supply Chain	Smart Grid & Infrastructure
Appropriate fallback solutions & safe modes	✓	✓	✓	✓	✓	✓
Leveraging physics, locality, and distance for authentication	✓	✓	✓			
Application of classic control theory to control those systems			✓	✓	✓	✓
Formal methods to incorporate security from the beginning	✓	✓	✓	✓	✓	✓
Developing benchmarks & metrics to evaluate security & safety	✓	✓	✓	✓	✓	✓
Security regulations & economic incentives	✓	✓	✓	✓	✓	✓
Design a privacy dashboard for users to understand their data	✓	✓	✓			
Model & secure the full lifecycle of IoT devices	✓	✓	✓	✓	✓	✓
Split design - leverage slower trusted parts to mediate technology executed in less trusted parts				✓	✓	

Figure 2. Overlap of Potential Novel Solutions to the Embedded Security Challenges of Each Application Area

DISTINGUISHING THEMES

- Several important distinctions were noted between the five application areas. A primary point of distinction is in the ownership of the system and the overall economic situation. For example, a smart home owner wants the ability to control the security and privacy of their personal life, while an autonomous vehicle owner may have to comply with more regulations due to the shared nature of roadways.
- The device manufacturer may claim ownership of some data as a way to improve the device performance. Modern data-driven businesses will want as much data as possible to optimize their systems for users and profit, as well as to protect against various threats. Ultimately, users should have rights to the data generated from their bodies and their behavior.
- In contrast, the data from critical infrastructure will be collected by local, state, and federal governments, as well as manufacturers and installers in order to monitor usage and design improvements to systems. Data from critical infrastructure will need to be protected from misuse but must be made available to those stakeholders who manage them.

DISTINGUISHING THEMES

- The role of regulations and incentives differs considerably across the five areas as well. Even within the area of medical and wearable devices, there is a huge range between FDA-regulated devices and the almost unregulated world of personal health apps on mobile phones.
  - The FDA, FTC or some other government agency should consider developing regulations for these new consumer devices and associated software.

- Incentives can be more effective than regulations in some embedded security solutions. As security and privacy become more visible and valuable to users, hopefully business incentives can play more of a role in setting security policy.

- Threat models also vary between application areas. Industry supply chains are threatened by counterfeits and recycled/repurposed parts that result in lost revenue and damage to brand reputation.

International and U.S. Agency Perspectives

INTERNATIONAL PERSPECTIVES PANEL

Yongdae Kim
Korea Advanced Institute of Science and Technology

Srdjan Capkun
ETH Zürich, Switzerland

Wenyuan Xu
Zhejiang University

Ross Anderson
University of Cambridge

INTERNATIONAL PERSPECTIVES ON THESE CHALLENGES

- Findings:
  - The major differences in government funding for embedded security between the USA and Asia/Europe is scale of opportunity (less in USA) and oversight (more overseas).
  - The USA may no longer have the global edge on embedded security research.
- Recommendations:
  - The USA can gain economic strength by ensuring that highly competitive embedded security research is funded, especially when the ideas are high risk and high reward.
  - Encourage international collaboration and do not discriminate basic research opportunities by citizenship so as to attract and retain talent in the USA that will likely foster entirely new marketplaces for societal benefit.

INTERNATIONAL PERSPECTIVES ON THESE CHALLENGES

- While much creativity exists in the USA, there are fewer opportunities to fund the proposed ideas than in countries such as Korea, China, and Switzerland.

- The USA is likely to lose its edge on leadership in embedded security and IoT security not because of willfully malicious actions of other countries, but more because of the stagnation of research funding for highly competitive proposals.

- In the last few years, many prestigious faculty have moved from the USA to Europe, China, and Canada.

MY WORKSHOP TAKEAWAYS (BY TOMAS VAGOUN)

- Grand Challenge
  - Develop integrated safety-security-privacy framework
    - Cyber-physical (& embedded) systems expose the need for a holistic approach to integrate safety, security, privacy, (+resiliency) requirements
- Research Priorities
  - Develop and leverage unique properties related to the physics and locality to improve security
  - Develop solutions for safe-mode/fallback operations
  - Advance methods to integrate security in real-time/concurrent systems
  - Advance split-ASIC and multi-chiplet design techniques
- Research Funding
  - The USA seems to be falling behind in funding embedded security research as compared to countries such as Korea, China, and Switzerland

REMINDER: TRUSTED MICROELECTRONICS IS A STRATEGIC ISSUE (BY TOMAS VAGOUN)

- Issue
  - Most COTS electronics used in the US, including those used by the DoD, are manufactured overseas—creating a significant security risk for the Nation from potential tampering
  - With large strategic investments (e.g., $150B by China, $100B by Saudi Arabia) and national subsidies, Asia is becoming the world-class center of microelectronics design and production, severely handicapping the US national security interests
- What actions are needed to reverse this trend?
  - Invest in innovative secure design solutions, which would allow the USG to use offshore state of the art commercial microelectronics capabilities, while satisfying the needs for trust
  - The secure design approach combines SW and HW assurance tools and verification capabilities to provide for trusted manufacturing outcomes
- Example
  - DoD Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC) Program
  - DoD to invest $2 billion in MINSEC between FY2019 and FY2023