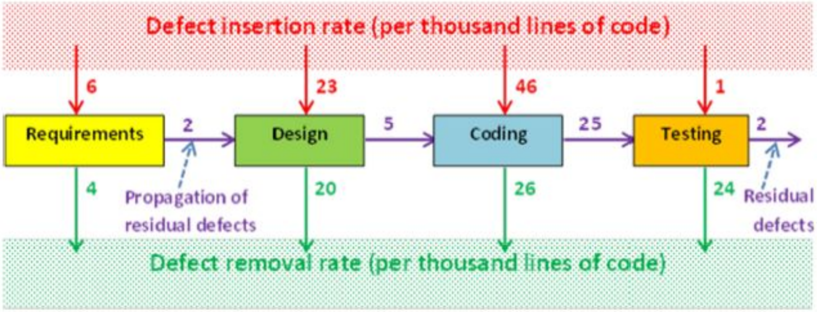
Report from ESCAR US – June 2018

Tomas Olovsson
Tomas.Olovsson@chalmers.se
Computer Science and Engineering

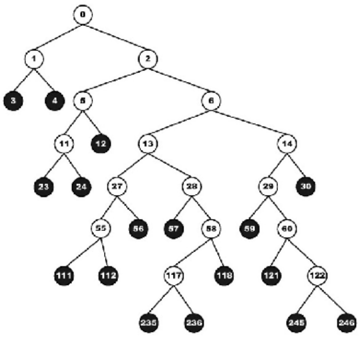
NASA Study on Flight Software Complexity

"Commissioned by the NASA Office of Chief Engineer, Technical Excellence Program, May 2009"


Defect insertion rate (per thousand lines of code)
6
23
46
1
Requirements
2
Design
5
Coding
25
Testing
2
4
Propagation of residual defects
20
26
24
Residual defects
Defect removal rate (per thousand lines of code)

65M lines of code ➔ 130,000 remaining defects

Hackers – Attack Trees



Attackers create “attack trees” – different paths attacks to reach their goals

Patching the symptom (e.g. #246) does not work

Compare with a Chess game:
Impossible to win with a bad opening

AutoSec

CHALMERS

Hacking the Law:
The Law and Economics of Bug Bounties

Amit Elazari – Ph.D. student, US Berkeley School of law

Researchers may face legal prosecution from the companies

Have to sign various non-disclosure agreements

Why are we attacking the attackers instead of letting them help us?

If they are not allowed to talk about the results, why should they bother?

AutoSec

CHALMERS

Examples from contracts

"Yahoo reserves the right to modify the conditions for the bug-bounty program at any time"

"TESTING MUST NOT VIOLATE ANY LAW, OR DISRUPT OR COMPROMISE AN DATA THAT IS NOT YOUR OWN"

→ the hacker is responsible for, for him/her, unknown problems

"attempt to gain unauthorized access, will be …";

"We reserve the right to forward details of the issue to third parties [to take action]".

Takeaways

Hackers want to play by the rules but the rules won't let them

For each type of bug found, describe:

- Kind of report wanted (for SQL, spoofing, …)
- Establish boundaries (to prevent damage, user privacy, use of compromised accounts)

Create a safe harbor to remove legal risks for them

If legal action is taken by a third party, the organization should protect the researcher

https://github.com/EdOverflow/legal-bug-bounty/blob/master/templates/safe_harbor.md

Efficient Reverse Engineering of Automotive Firmware

Alyssa Milburn and Niek Timmers – Riscure

1. Obtain/extract code
   - eeprom, debug interfaces, vulnerabilities to dump code, hardware attacks
   - Not that difficult
2. Analyze code
   - Code complexity is the challenge, function call graph huge
   - Use emulator to emulate: input, CAN controllers, interrupts and timers
   - Simulate input by placing it into buffers → identify input buffers, output buffers, key storage, IDS handling
   - Follow data through the system and taint all data it comes in contact with

Takeaways

Reverse engineering not that hard

Emulator decrypts firmware if encrypted

You can’t hide secrets in firmware. Use secure hardware storage (TPM)

If standard operating systems are used – tools already available to everyone

Automotive Exploitation Sandbox: A Hands-on Educational Introduction to Embedded Device Exploitation

Nathaniel Boggs – Red Balloon Security

Goals:

- Use remote hackers to find bugs in systems
- Provide hands-on platform for hacking real hardware
- Helps to understand attack chains

Setup:

- Internet connected ECUs to be allocated by hacker
- Reset every *n* minutes
- Demonstrated attacks against a QNX microkernel on a development board

Automotive SOC - Concept Description

Liron Kaneti – Argus Cyber Security Ltd.

How do we know that some vehicular accidents are related and should be investigated?

- New area, hard to collect data to find correlations
- Built-in vehicle analysis needed -> Only 10 Mbyte data/vehicle/year

A-SOCs, Automotive Security operations centers needed

- Real-time response to incidents

Focus on fleet immunization, containment and first response for vehicles on the road

- Similar to error-shutdown in other areas

Online Detection of Anomalies in Vehicle Signals using Replicator Neural Networks

Marc Weber – Karlsruhe Institute of Technology + Vector

Signature-based IDS systems cannot detect new attacks

- Also require frequent updates (like anti-virus systems)

Anomaly-based IDS: problem with high false positive rate (FPR)

- One false alarm/year/vehicle… with millions of vehicles…

Developed an anomaly-based IDS system

- Input sent to machine-learning platform
- Evaluated three different types of such systems
- Selected one with a sliding window with 4 samples

60-70% TPR and 0,065% FPR

Automotive Evidence Collection - Automotive Driving Aids and Liability

Vlad Gostomelsky – Spirent Federal

1. GPS spoofing can be fatal
   - Human drivers have been driving into lakes when the navigator tells them to…
   - Jammers available for $18 on eBay
   - Spirent sell commercial jammer detectors
2. Event data recorders important
   - Data modification or deletion must be addressed
   - Recorders should cut off all power after crash
   - Tamper-proof hardware needed

CommPact: Exploring the Feasibility of Autonomous Vehicle Contracts

Jeremy Erickson – University of Michigan

How to generate contracts between vehicles

- Platooning: "keep speed x"
- Necessary to be able to break contracts fast enough
- Consensus important

Argued that they can solve problem when all hardware is malicious

- And when communication fails to some vehicles
- Details were missing…

Don't aim for full synchronization – impossible

- "For braking, only require that a vehicle starts to brake at the same time or before the vehicle in front"

Robust Physical-World Attacks on Deep Learning Visual Classifiers

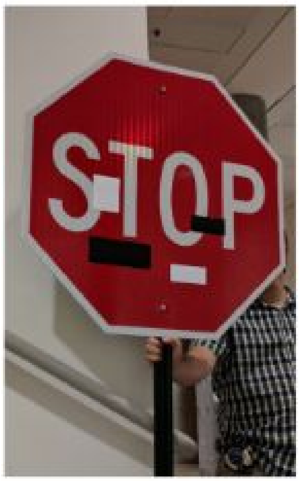
Prof. Atul Prakash – University of Michigan

Small stickers attached to a stop sign caused a vision system to misidentify it as a Speed Limit 45 sign!

The problem is harder than it may look:
angle, distance, lighting, color reproduction, confusing backgrounds, shadows, dirt, stickers and camera noise

Machine learning algorithms used, but are hard to control

Attacks will always make use of design flaws and design shortcomings



Cryptographic Algorithm Standards for Commercial Applications in China

Junfeng Fan – Open Security Research, Inc.

APPROVED

Managed by OSCCA

- Office of State Commercial Cryptography Administration
- Similar to NIST
- Crypto-products free to use, certificate shows customers standard compliance
- Likely vehicle manufacturers need to provide this

Crypto algorithms standardized (SMnn)

- SM2 = ECC; SM3 = Hash functions; SM4 = Block Ciphers
- Also standards for Randomness test and cryptography test criteria

State of the art standards – may become ISO/IETF standards

- SM2 and SM9 (identity-based cryptography) added to ISO/IEC 2017

Alternate Modality: Cross Pollinating Cyber Security Lessons Between Maritime, Rail, and Automotive

Nate McFeters, Jim McKenney – NCC Group, Alex Soukhanov – Moran Shipping

Rail:

- Trains are becoming fully connected and remotely controlled
- Security way behind automotive sector

Maritime:

- Standardized messages simplify attacks (NMEA 2000 – CAN)

Comparison with automotive:

- All use CAN
- But staff trained for critical situations when systems fail
- Software escrow → always possible to fix problems
- More redundancy than in vehicular systems
- IMO (Maritime Organization) will require cyber-security functionality 2021 for ships to be sea-worthy

Clock Phishing Attack on Clock Based Intrusion Detection Systems for CAN Protocol

Hafiz Malik – University of Michigan

Many papers describe how to, on the physical layer, detect which ECU is transmitting:

- Check the timing for ECU transmissions and estimate each ECU's clock skew to detect if another ECU forges messages

It is possible for a compromised ECU to learn the behavior of the clock and they provide a demo on YouTube.

AutoSec

CHALMERS

Fault Injection on Diagnosis Protocols

Niek Timmers - Riscure

Proposal: Inject faults to bypass security

if (authenticated) then ….

Method: Run ECU outside specified voltages or frequencies, create glitches

UDS (Unified diagnostic services), ISO 14229 useful target

- Often used for "secure" firmware updates
- Demonstrated it is possible to bypass secure boot [Blackhat demo]

Message: Use fault injection in your own testing

- And write code that require two or more glitches to fail!

AutoSec

CHALMERS

Conclusions

Many interesting papers:
cyber-security – attacks – countermeasures – IDS systems – legal issues – crypto standards – attack demonstrations

Slides from presentations and papers available on Escar website

AutoSec

CHALMERS