CODENOMICON

“The story of how I hacked into your TV”

Rikke Kuipers

Agenda for today

- Intro into fuzzing
- Changes in electronic landscape
- Case study: Televisions
- Case study: Network Attached Storage
- Solving the problem

CODENOMICON

$ whoami

- Background in networking
- Huge interest in IT security
- Security research
- Breaking things for fun and (not so much) profit.

CODENOMICON

The fuzz about fuzzing

- Modern security testing is about finding unknown zero-day vulnerabilities in devices and software before and after release
- Provides a quick technique for security assurance for any device or software

CODENOMICON

Different techniques

- Random fuzzing
- Block-based fuzzing
- Model-based fuzzing
- Traffic capture fuzzing

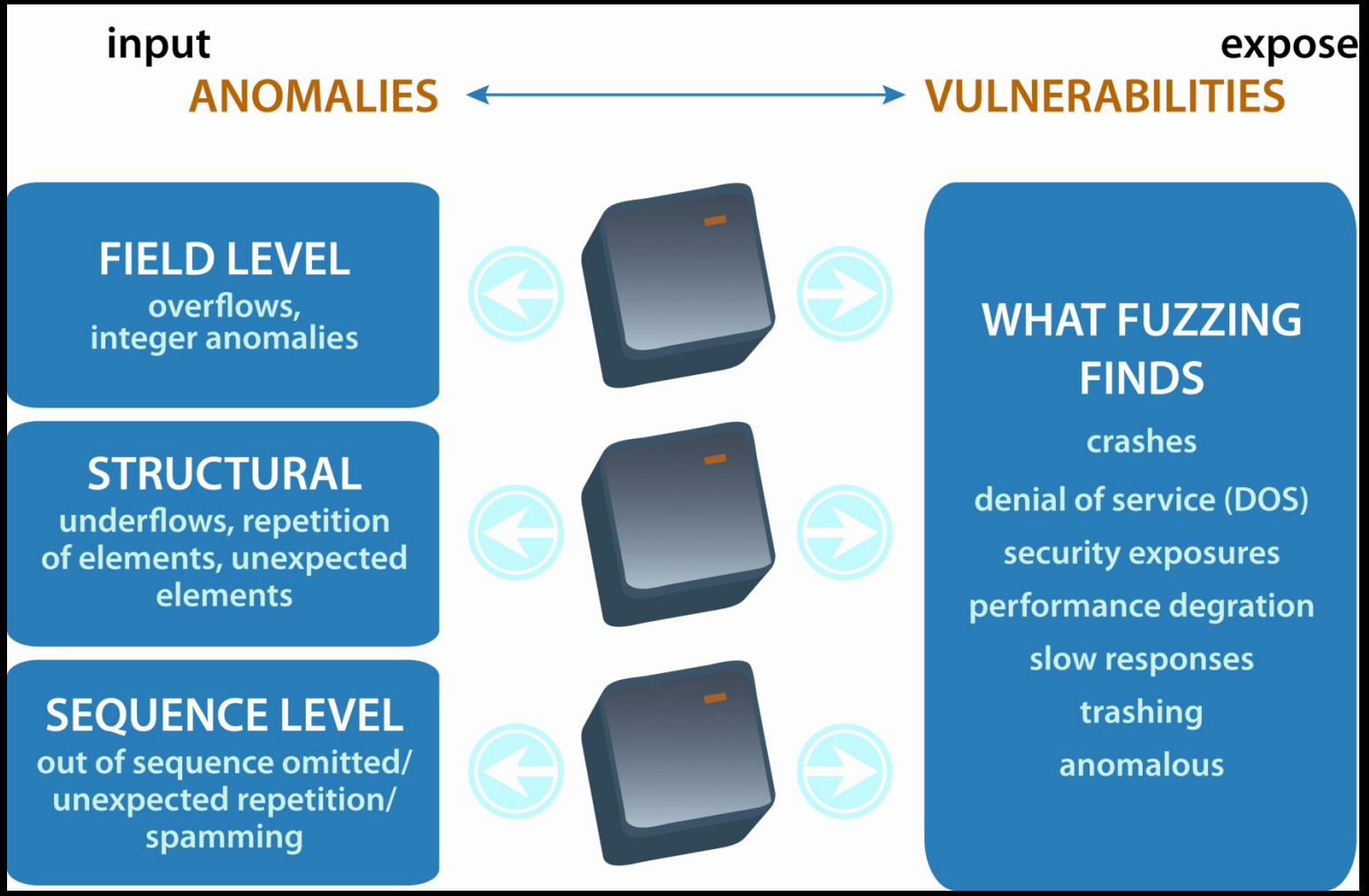
CODENOMICON

History of Fuzzing

- **1990** Random fuzzing becomes popular. Hackers use Fuzzing for zero day discovery;
- **1999** Model-based fuzzing becomes popular. Most of the zero-days found with fuzzing;
- **2001** Network equipment manufacturers start using Fuzzing for protection against hackers;
- **2006** Telcos integrate Fuzzing into acceptance testing and test for zero-day threats;
- **2010** Large-scale propagation of Fuzzing at
  - Finance
  - Government
  - SCADA
- **?** Fuzzing is part of the Acceptance Criteria

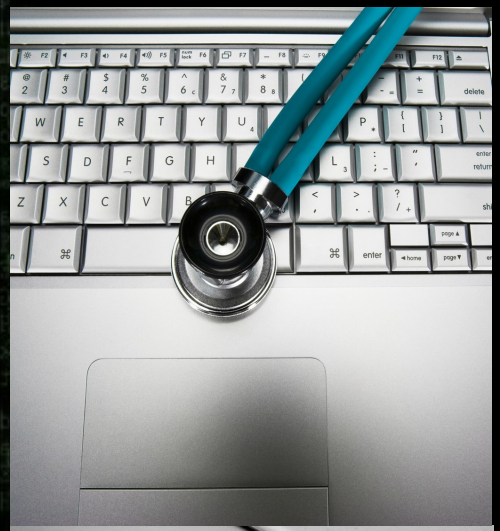
CODENOMICON

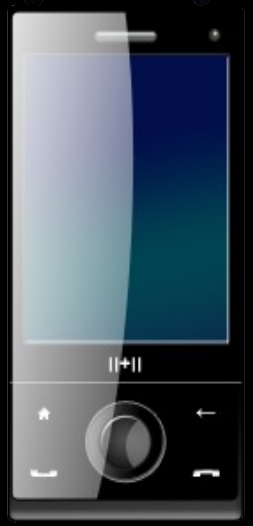
What can be found?

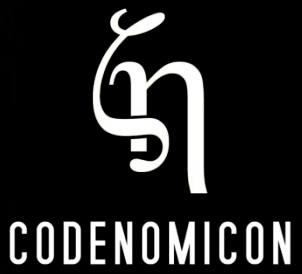


CODENOMICON

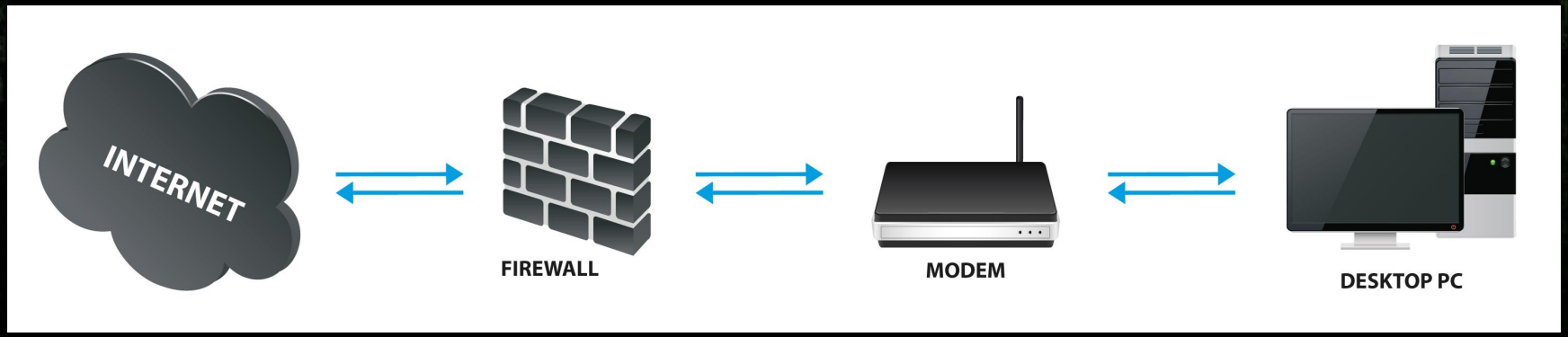
Changing landscape





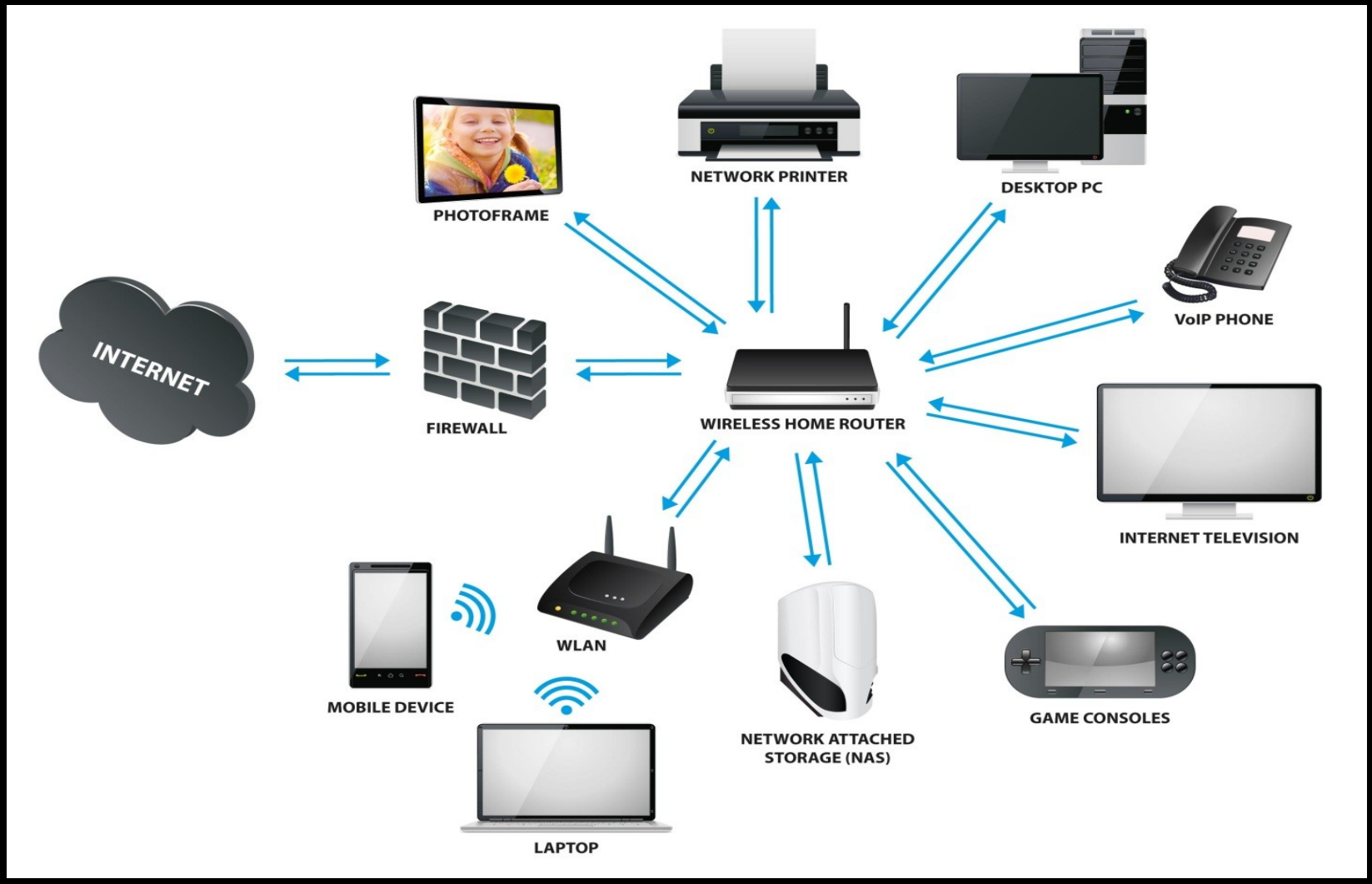


Traditional consumer environment



CODENOMICON

Modern consumer environment



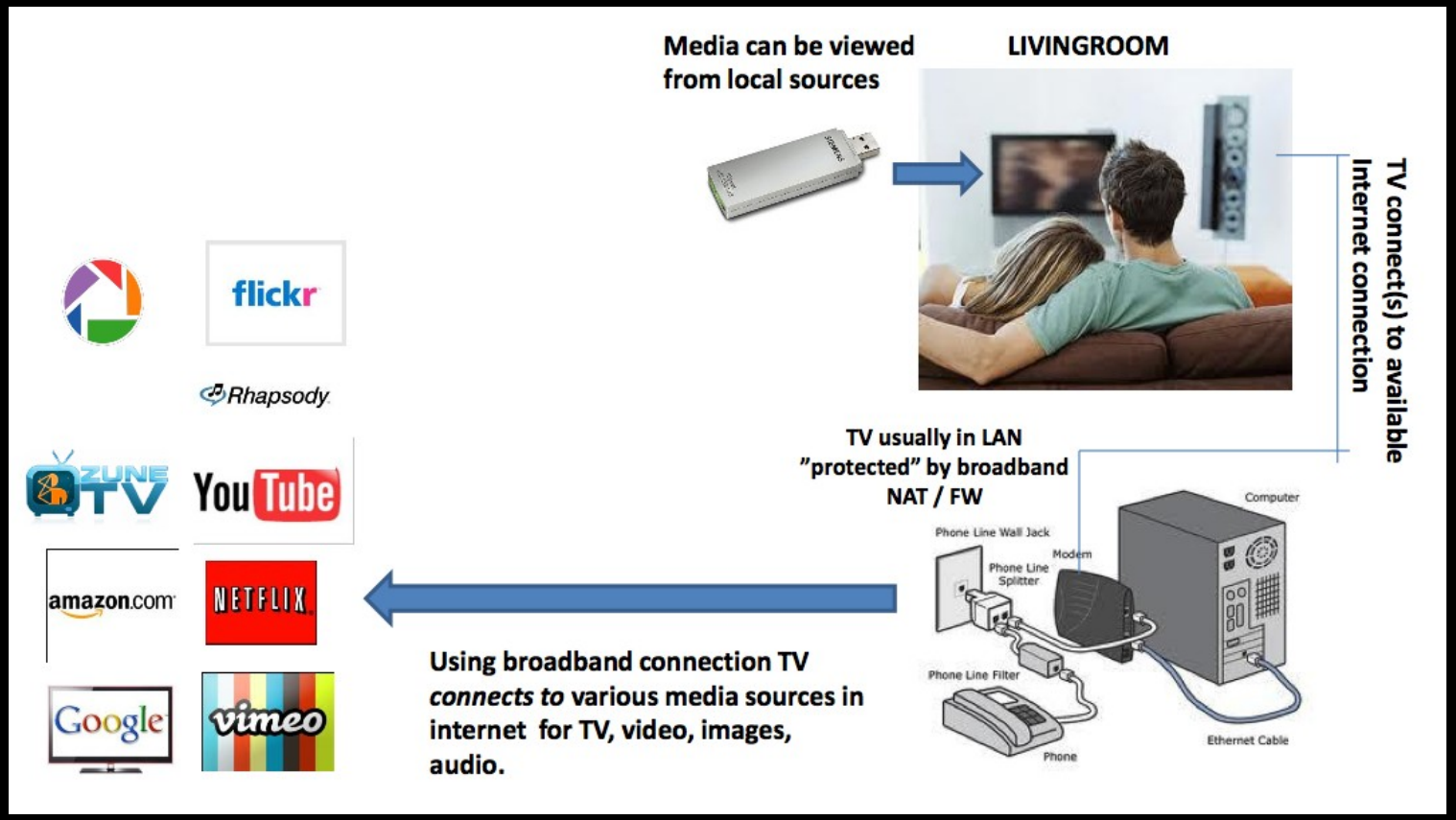
CODENOMICON

Case study: Televisions

- Dumb TVs
- Media center TVs
- Internet enabled TVs

CODENOMICON

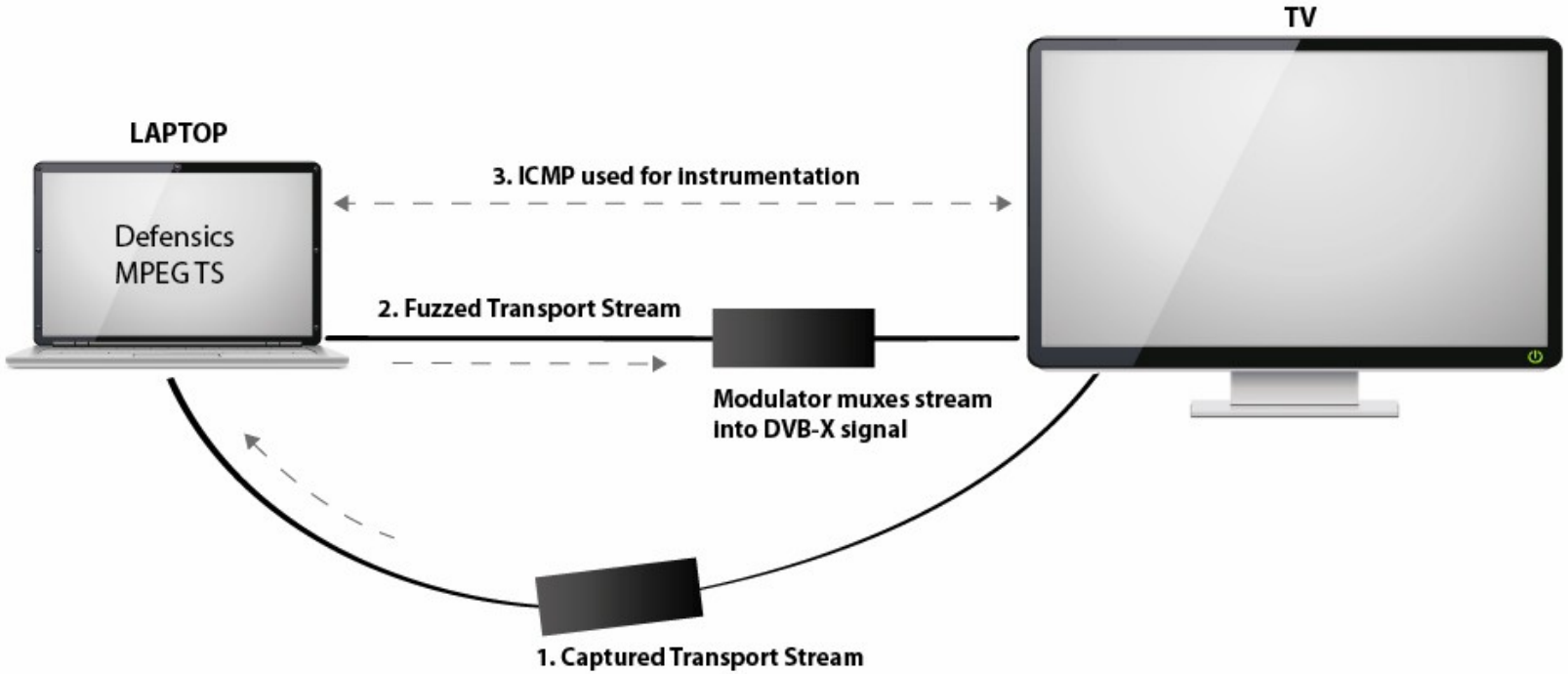
What's in there?



Attack surface

CODENOMICON

What? DVB Fuzzing!

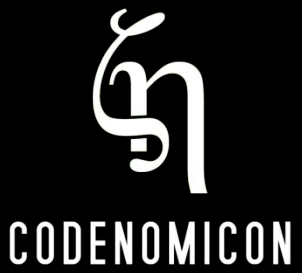



CODENOMICON
Console ports <3
Manufactured under license from Dolby Laboratories. "Dolby" and the double-D symbol are trademarks of Dolby Laboratories.
HDMI / DVI IN
3
2
1(DVI)
AUDIO IN (RGB/DVI)
OPTICAL DIGITAL
AUDIO OUT
RGB IN (PC)
RS-232C IN (CONTROL & SERVICE)
COMPONENT IN
VIDEO
AUDIO
AV1 (RGB)
AV2
ANTENNA IN
TruSurround XT, SRS and symbol are trademarks of SRS Labs, inc.

CODENOMICON

Possible threat scenarios

- Targeted attack using a directional antenna
- Or: why think directional if you can think omni-directional?
- Important game on TV? Time to buy airtime!
- Youtube, Facebook, Google+, etc



Case study: Network Attached Storage

- Basically a headless server
- High profile target for attackers
- Attack surface is large
- Who updates these (and why you maybe also shouldn't..)

CODENOMICON

Protocol	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Vendor 5
Ethernet	PASS	PASS	PASS	FAIL	FAIL
ARP	PASS	N/A	PASS	PASS	PASS
IPv4	FAIL	FAIL	FAIL	PASS	FAIL
ICMPv4	PASS	PASS	N/A	N/A	PASS
TCPv4	FAIL	PASS	FAIL	FAIL	PASS
HTTP	FAIL	PASS	PASS	PASS	PASS
FTP	FAIL	FAIL	FAIL	FAIL	FAIL
TLS	N/A	N/A	N/A	N/A	PASS
NetBIOS	PASS	FAIL	PASS	PASS	FAIL
CIFS	N/A	FAIL	FAIL	N/A	N/A
SMB2	N/A	N/A	N/A	N/A	FAIL
NFS	PASS	N/A	N/A	N/A	N/A
UPnP-GENA	FAIL	N/A	FAIL	N/A	FAIL
UPnP-SOAP	FAIL	PASS	FAIL	N/A	FAIL
UPnP-SSDP	PASS	FAIL	PASS	N/A	PASS
UPnP-Connmanager	N/A	FAIL	N/A	N/A	N/A
UPnP-SOAP Layer 3 Forwarding	N/A	PASS	N/A	N/A	N/A
80211-AP	N/A	FAIL	N/A	N/A	N/A
80211-WPA-AP	N/A	PASS	N/A	N/A	N/A

CODENOMICON

King of the hill..

WIRELESS (GPRS, EDGE/3G): GSM, SMS, MMS, SMIL, OTA updates, ...

WIRELESS (802.11): 802.11a/b/g/n, WPA, WPA2, ...

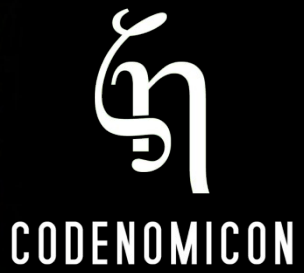
WIRELESS: Bluetooth: L2CAP, RFCOMM, SDP, OPP, A2DP, AVRCP, PBAP, DUN, ...

IP CONNECTIVITY: IPv4 (ARP, ICMP, IGMP, IP, UDP, TCP), IPv6 (IP, ICMP, ND, RD, SEND, MLD, TCP, UDP), HTTP, TLS/SSL, OCSP, RTSP, SIP/IMS, RTP/RTCP, SigComp, DNS, MDNS, DHCP, NTP , SOAP, REST/JSON, SMTP, POP3, IMAP4, WAP/WMLC, ...

PHYSICAL CONNECTIVITY: USB, SERIAL, MEMORY CARD, SIM, ...

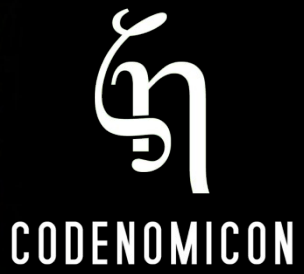
[WEB] APPLICATIONS: XML, DRM, HTML5 (CSS, HTML, Javascript) , AT commands, inter process APIs / RPCs, ...

MEDIA: AUDIO (AAC, MP3, MP4, 3GP, WAV, ...), IMAGES (JPG, GIF, PNG, TIFF, ...), VIDEO (MPG1, MPG2, MP4/H.264, WEBM,...), ARCHIVES (ZIP, JAR, CAB, ...), DOCUMENTS (PDF, DOC, PPT,..), X509, EMAIL (MIME, calendar, vcards,...), DRM, Flash, Java classes , Application installers, ...



Lessons Learned in Fuzzing Embedded “Smart” Devices

- Outside vendor environments comprehensive testing near impossible in meaningful time
  - Hackers go for the low hanging fruits, and always find flaws
- Therefore vendor/integrator tests need careful planning:
  - Test the easier to test interfaces first
  - Test for the baseline (good enough test)
  - Push testing up the production line (vendors, contractors)
- Automation of tests is essential
  - Testing process may not be portable across teams
  - Black-box testing is often the only solution



And they all crashed forever happily after..

- Download our whitepapers (if interested..)!
- Questions?

Merci beaucoup!