Digital Investigations for IPv6-Based Wireless Sensor Networks

By

Vijay Kumar, George Oikonomou, Theo Tryfonas, Dan Page and Iain Phillips

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

University of BRISTOL

Digital Investigations for IPv6-Based Wireless Sensor Networks

V. Kumar, **George Oikonomou**, T. Tryfonas,
D. Page and I. Phillips

University of BRISTOL

How to Retrieve Network Data from Wireless Embedded Devices

University of BRISTOL

Tiny, Tiny, Tiny

- TI CC2530 SoC: Smaller than a dime

- 8-bit, 8051-based micro
- 8KB RAM
- 256KB Flash

- Can run TCP/IP – IPv6

University of BRISTOL

Operating Systems

- **Contiki**
  - 8-, 16-, 32-bit micros
  - 8 – 32 KB RAM
  - < 512 KB Flash
  - Dozens of supported platforms (official and unofficial)
- TinyOS
- …

University of BRISTOL

Outline

- **Motivation – Introduction**
- Extraction
- Analysis
- Correlation
- Open Issues – Further Work

University of BRISTOL

GINSENG (FP7)

- Mission-critical applications
- Operational oil refinery

- Contiki-powered nodes
- Bespoke network stack

O'Donovan et al. "The ginseng system for wireless monitoring and control: Design and deployment experiences" ACM Trans. Sen. Netw., 10, 4:1–4:40.

University of BRISTOL

Commercial Products

- Contiki-powered products at CES 14

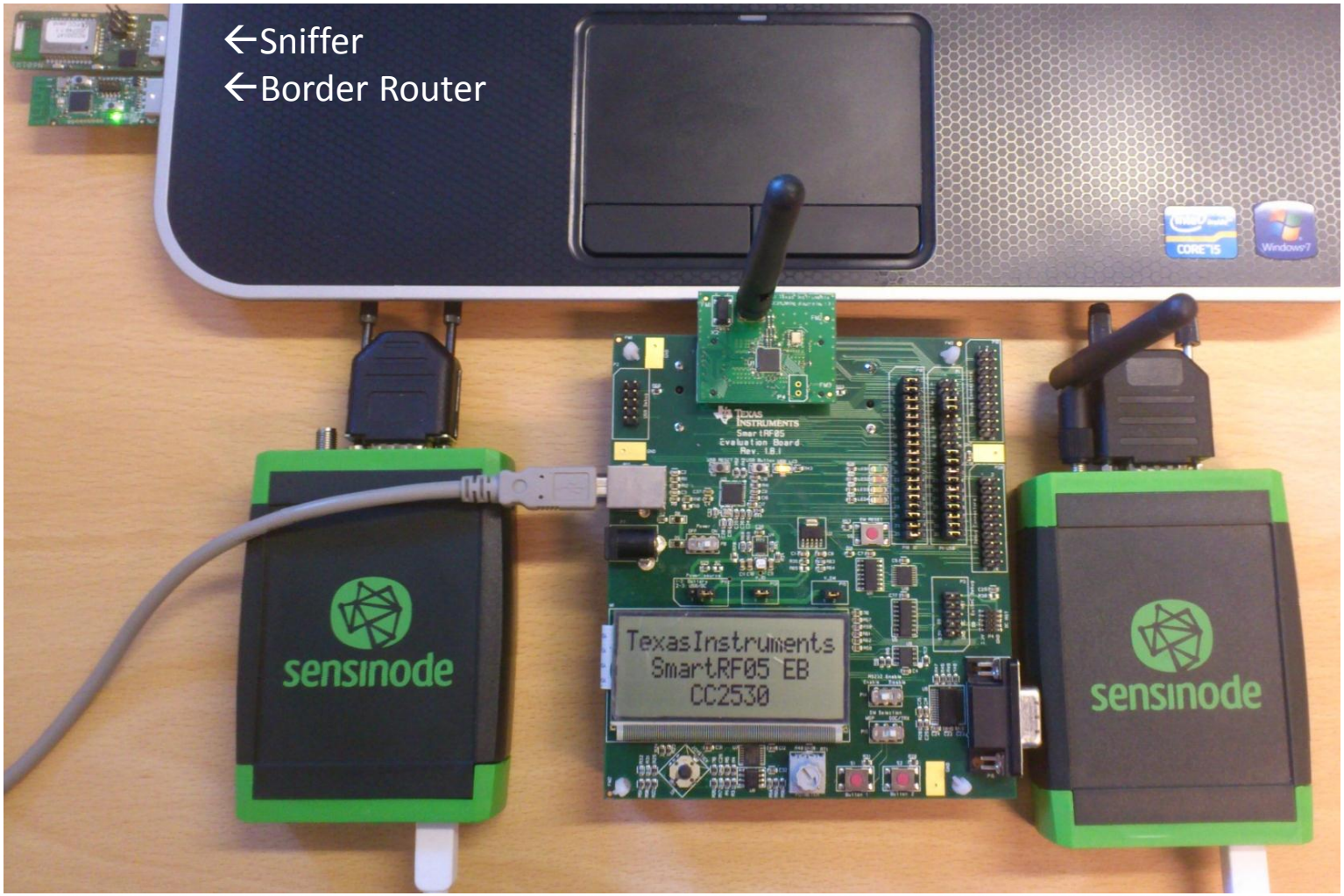
http://contiki-os.blogspot.co.uk/2014/01/contiki-products-at-ces-2014.html

- Hacked smart objects

http://www.bbc.co.uk/news/technology-28208905

University of BRISTOL

Kit



University of BRISTOL

This Work

- Recovery of networking information
  - Routing tables
  - Routing protocol metadata
  - Neighbor Discovery (ND) Cache
  - …
- Network topology reconstruction

- Focus on TI CC2530
  (+ older CC2430: big similarities = quick win)
- RAM Extraction and analysis

University of BRISTOL

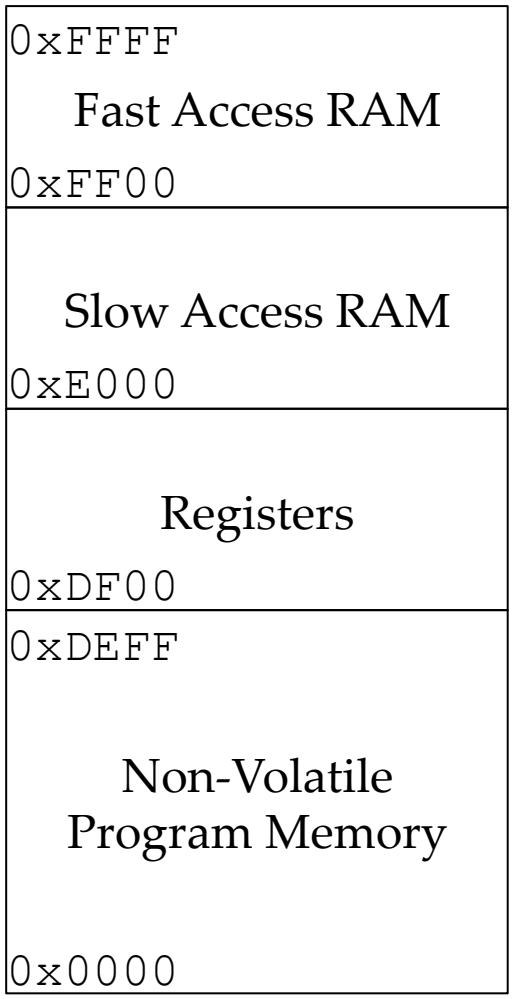
Memory

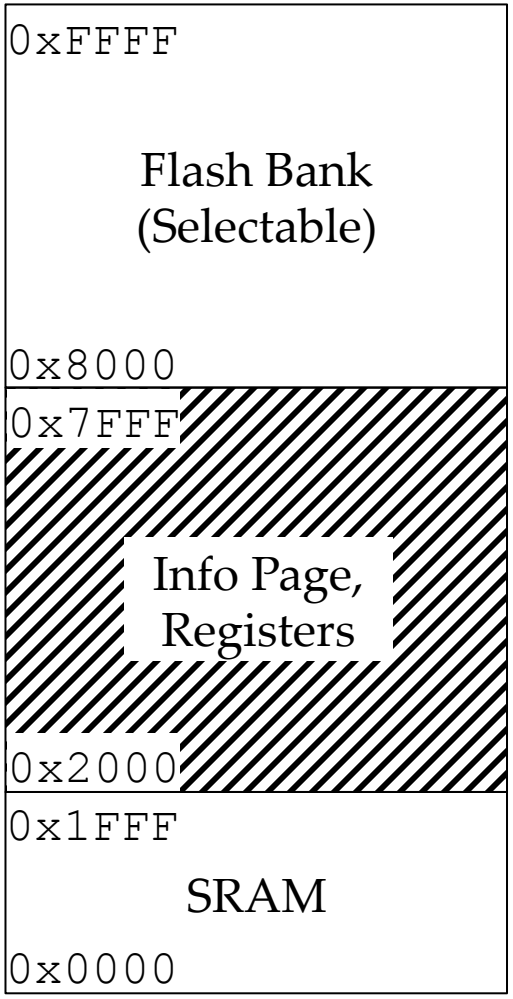
- 8051 MCU – Harvard-based Architecture
  - Separate Code and Data Memory Spaces
- Physical Memory:
  - Flash
  - SRAM
  - Registers
- Memory Spaces (Distinct, Partially Overlapping)
  - CODE: Instruction memory (Flash)
  - DATA: Fast access, 256 bytes data (SRAM)
  - SFR: Registers
  - XDATA: SRAM + Flash + Registers, 64 KB, Slower Access

University of BRISTOL

XDATA Space

CC2430



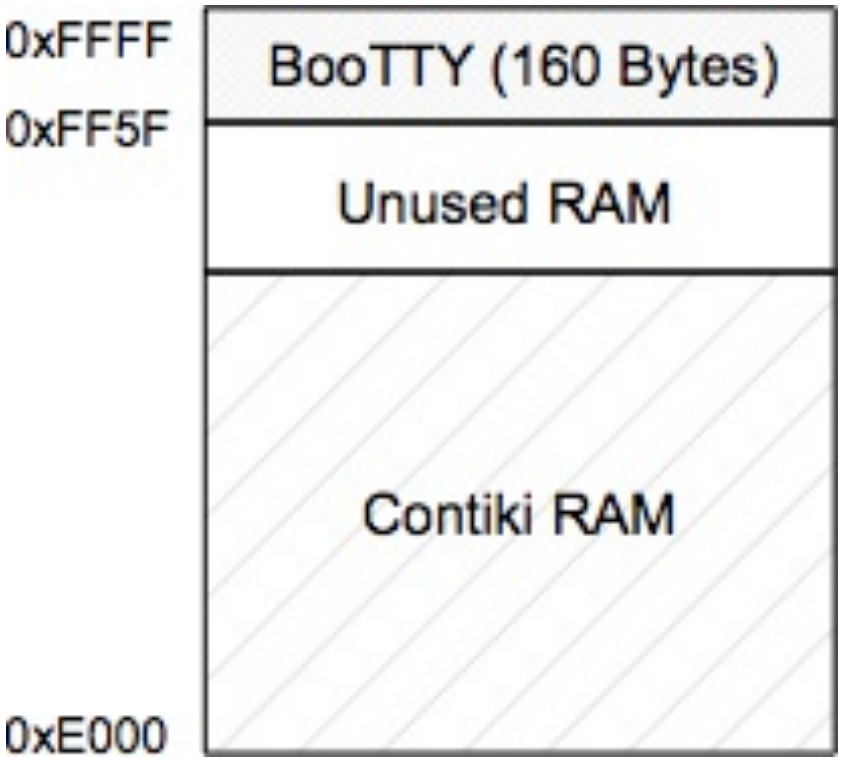


CC2530

University of BRISTOL

Extraction

- Over the debug interface
  - CC2530 (cc-tool)
- Over UART with a bootloader
  - CC2430
- Don’t trash the RAM!



University of BRISTOL

EUI-64 and IPv6

- An EUI-64 Identifier (8-byte MAC)

`00:15:20:00:00:02:20:EB`

- A Link-Local IPv6 Address (LL IPv6)

`FE80:0000:0000:0000:0215:2000:0002:20EB`

`FE80::0215:2000:0002:20EB`

- A Routable IPv6 Address (Unique-Local)

`FD4D:4267:5F8C:0000:0215:2000:0002:20EB`

`FD4D:4267:5F8C::0215:2000:0002:20EB`

EUI-64 and IPv6: On RAM

EUI		00 15 20 00 00 02 20 EB
LL IPv6	[8 bytes]	02 15 20 00 00 02 20 EB
UL IPv6	[8 bytes]	02 15 20 00 00 02 20 EB

Observations:

1. Interface ID derived from EUI-64 with 1 bit inverted (the U/L bit)
2. One link-local and one routable v6 same If ID

University of BRISTOL

Analysis

- Find all 16-byte block occurrences of:
  `FE 80 00 00 00 00 00 00 [ If ID ]`
  Gives us a list of 8-byte `[ If ID ]`s
- For each `If ID`, find all 16-byte blocks:
  `[ not FE80:: ] [ If ID ]`
  first 8-bytes of each match are a candidate network prefix `(PREFIX)`
- For each `PREFIX`, search for 16-byte block occurrences of:
  `[ PREFIX ] [ any 8 bytes ]`
  more candidate IPv6 addresses

University of BRISTOL

Analysis

3 full passes across entire RAM, very quick

We now have:

- List of candidate IPv6 addresses on RAM
- For each of those, invert the U/L bit in `[ If ID ]`
- List of candidate EUI-64s present on RAM

University of BRISTOL

Data Types

Listing 1: An entry in Contiki's ND Cache

```
typedef struct uip_ds6_nbr {
  uint8_t isused;
  uip_ipaddr_t ipaddr;
  uip_lladdr_t lladdr;
  /* Meta Data */
} uip_ds6_nbr_t;

uip_ds6_nbr_t uip_ds6_nbr_cache[SIZE];
```

Listing 2: An entry in Contiki's Default Routes Table

```
typedef struct uip_ds6_defrt {
  struct uip_ds6_defrt *next;
  uip_ipaddr_t ipaddr;
  struct stimer lifetime;
  uint8_t isinfinite;
} uip_ds6_defrt_t;
```

Listing 3: Extract of the RPL parent data structure

```
struct rpl_parent {
  struct rpl_parent *next;
  struct rpl_dag *dag;
  rpl_metric_container_t mc;
  uip_ipaddr_t addr;
  rpl_rank_t rank;
  /* more fields */
};
```

Listing 4: An entry in Contiki's Routing Table

```
typedef struct uip_ds6_route {
  struct uip_ds6_route *next;
  uip_ipaddr_t ipaddr;
  uip_ipaddr_t nexthop;
  /* more fields */
} uip_ds6_route_t;
```

- Knowledge of Data-Types
- No knowledge of data structure memory address

University of BRISTOL

Example: ND Cache

Statically pre-allocated array of entries:

- Each one is a `struct uip_ds6_nbr`
- Fixed length
- Strict pattern:

```
01 [ LL IPv6 ] [ EUI-64 ] [ meta ]
```

We don’t need to parse, we already have a list of all EUI-64s + their locations

University of BRISTOL

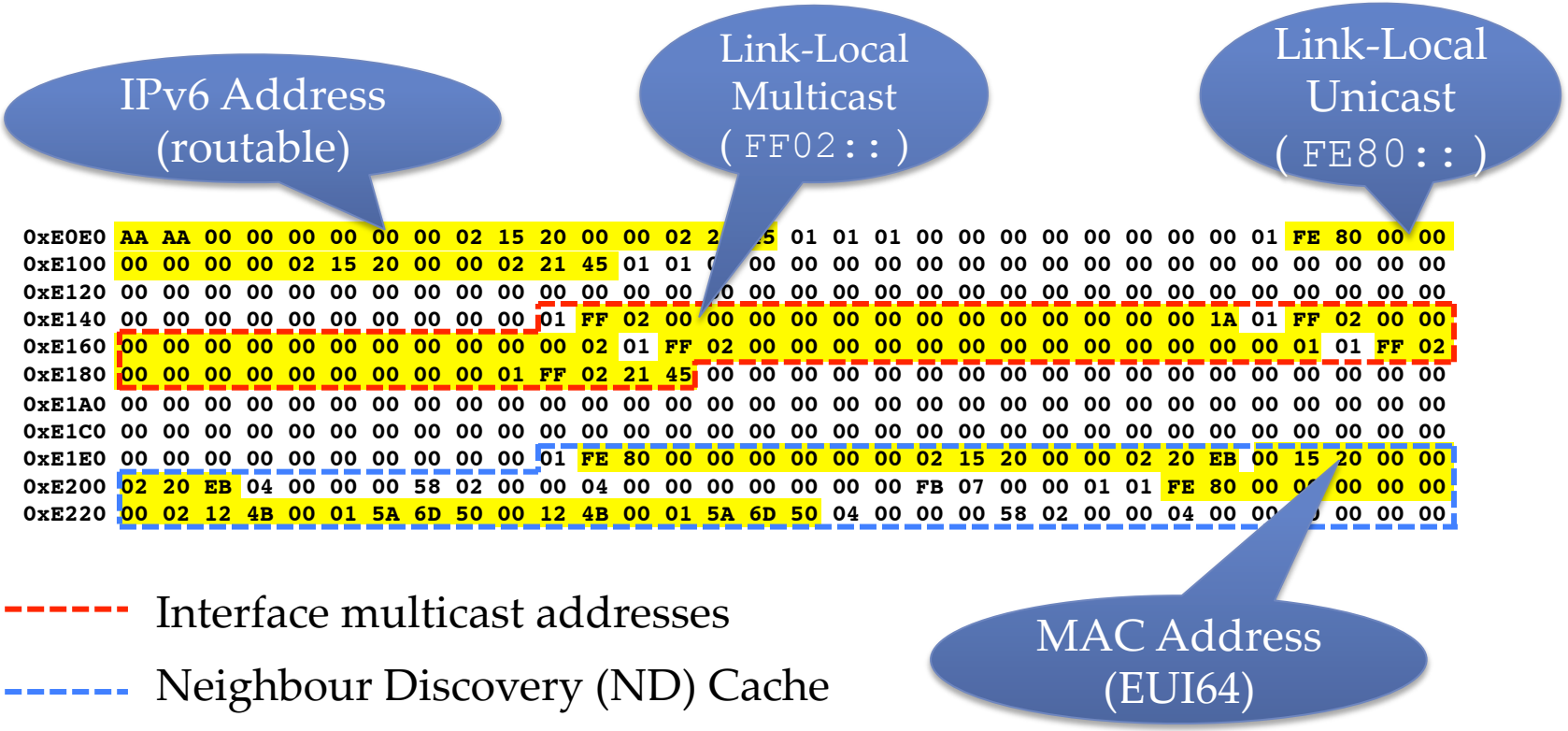
Smooth Sailing

- Node's own IPv6 addresses and EUI-64
- Routing table
- Default route (stored separately)
- RPL:
  - Parents
  - Instance table
  - DODAG info
- Interface info, multicast addresses

University of BRISTOL

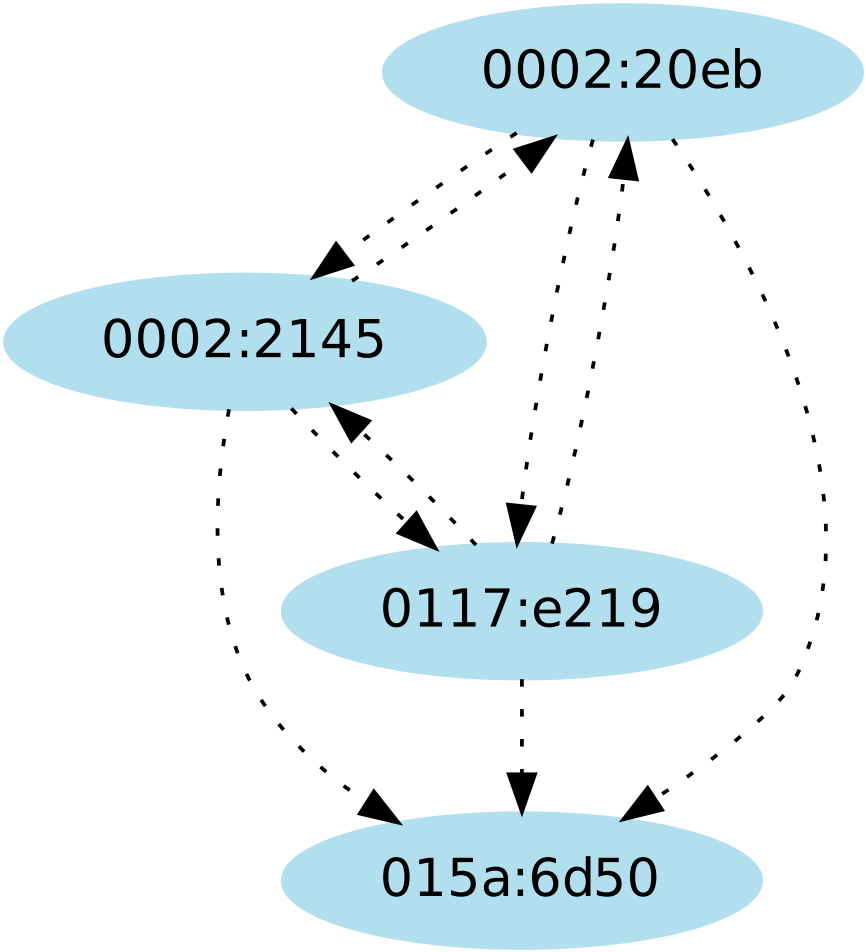
RAM Analysis

RAM Contents of an 8051-based Micro Powered by a Contiki Firmware



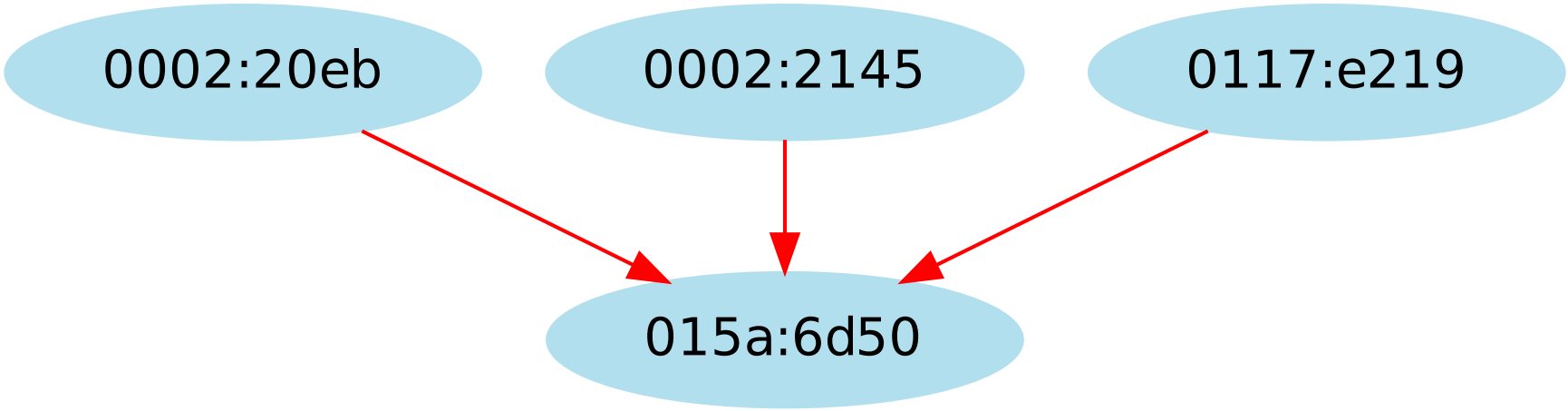
University of BRISTOL

Link Layer



University of BRISTOL

Network Layer



University of BRISTOL

Open Issues

- Data loss after device resets:
  - RAM retention characteristics
  - Data structure initialization at startup
- Locked debug bits

University of BRISTOL

Future Work

- More OS versions
- More architectures (Arm CM3, msp430)
- Large-Scale Networks
- Forensic Readiness

University of BRISTOL

ForToo

- Digital forensics for emerging technologies
- Smartphones
- Social networks
- Internet of Things

This work has been supported by the European Union's Prevention of and Fight against Crime Programme "Illegal Use of Internet" - ISEC 2010 Action Grants, grant ref. HOME/2010/ISEC/AG/INT-002.

University of BRISTOL

Thank You!

g.oikonomou@bristol.ac.uk

University of BRISTOL

Data Loss

Device and Use-Case	Device not Reset	Device Soft-Reset	Device Power-Cycled
Sensinode N740			
Bootloader Pre-Installed	Success		Partial
Bootloader Installed by Investigator	Partial	Partial	Failure
SmartRF05EB + CC2530EM	Success	Data Overwritten	Data Overwritten

University of BRISTOL

RERUM

Security, Privacy, Reliability for the IoT

- FP7 STREP: Grant nº 609094
- Start: 1st September 2013
  Duration: 36 months
- Total Cost: €5,196,176.00
- Consortium:
  - 12 partners from 6 countries
  - 2 Local Authorities
- https://ict-rerum.eu

This project has received funding from the European Union's Seventh Programme for research, technological development and demonstration under grant agreement nº609094.

University of BRISTOL

GINSENG (FP7)