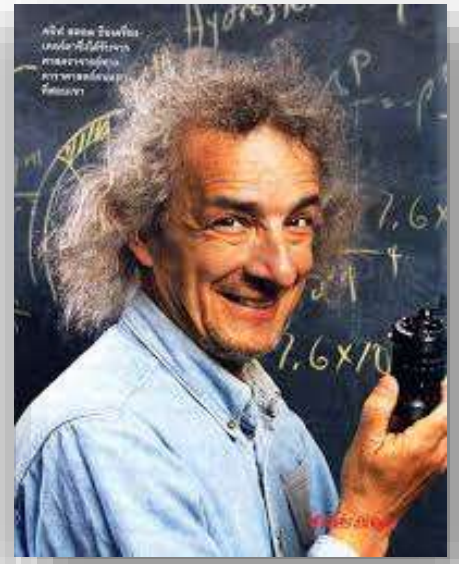
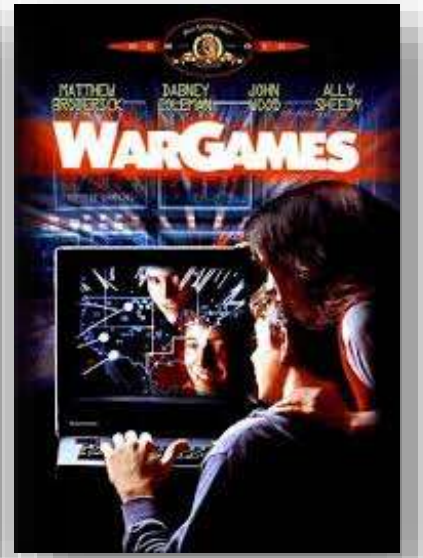
R. Stallman *C. Stoll* *S. Wozniak* *1983*



WHAT EVERY HACKER USED TO KNOW, A WALK DOWN HISTORY LANE

Guy Barnhart-Magen,

July 4, 2017

BSIDES TLV

LEGAL NOTICES AND DISCLAIMERS

This presentation contains the general insights and opinions of Intel Corporation (“Intel”). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

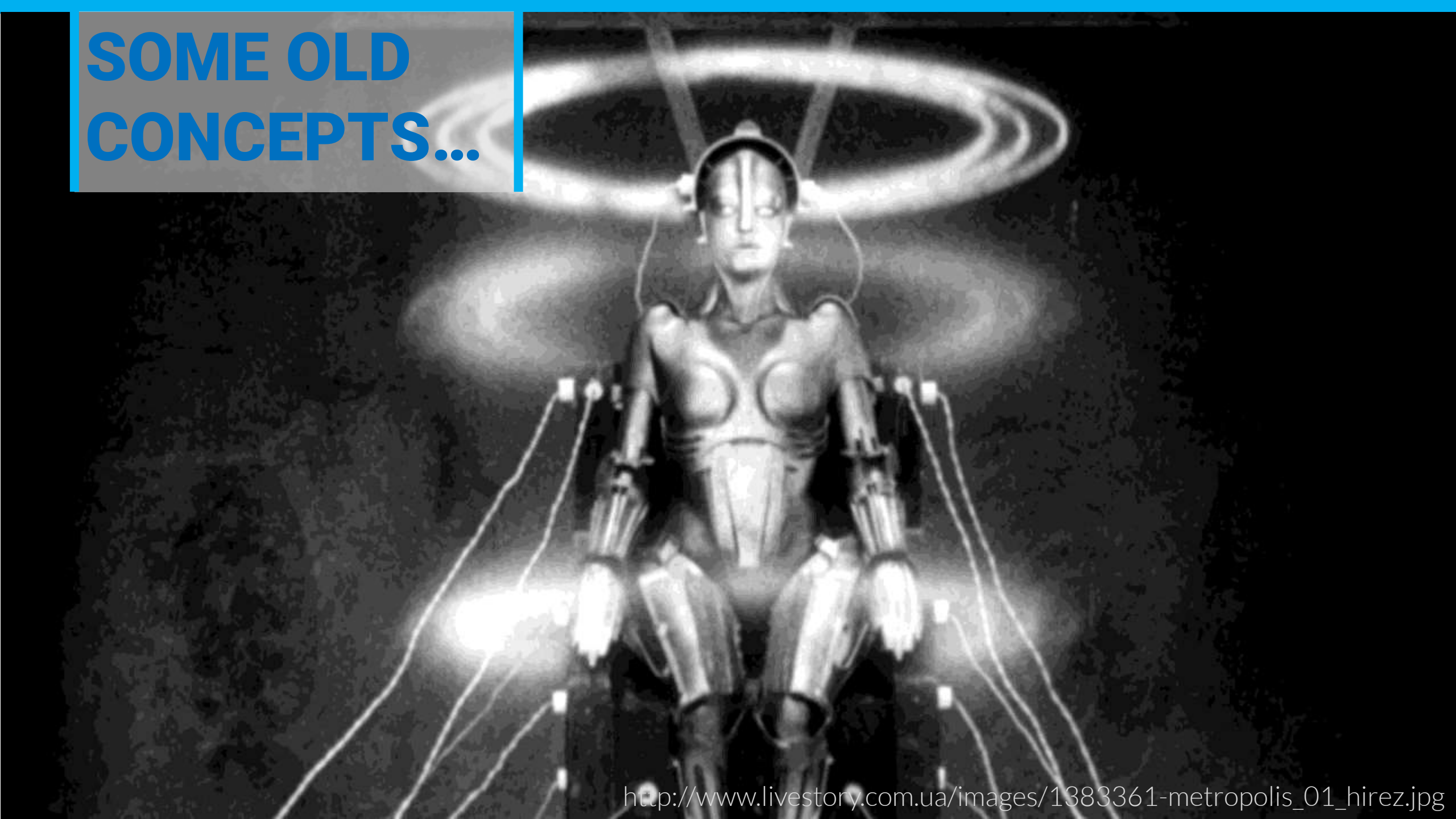
No computer system can be absolutely secure.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

WHO AM I?

- Guy Barnhart-Magen
- **Security Researcher**,
  Manager, Presenter
- Worked in:
  - 3 Startups, 3 Corporates
- iSTARE team
  - Intel Security Threat Analysis and Reverse Engineering
- “We break what we make”

SOME OLD CONCEPTS...

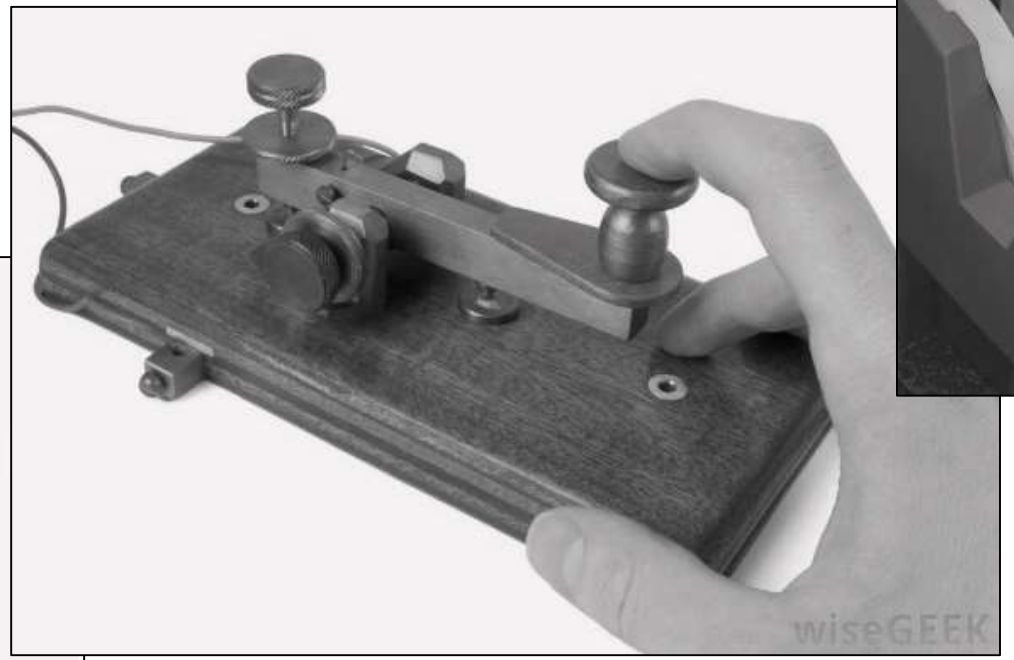


http://www.livestory.com.ua/images/1383361-metropolis_01_hirez.jpg

A DIFFERENT WAY TO COMMUNICATE

- Text based
- Chat channels
- Private channels
- Share files, images

TTY = Teletype Emulation



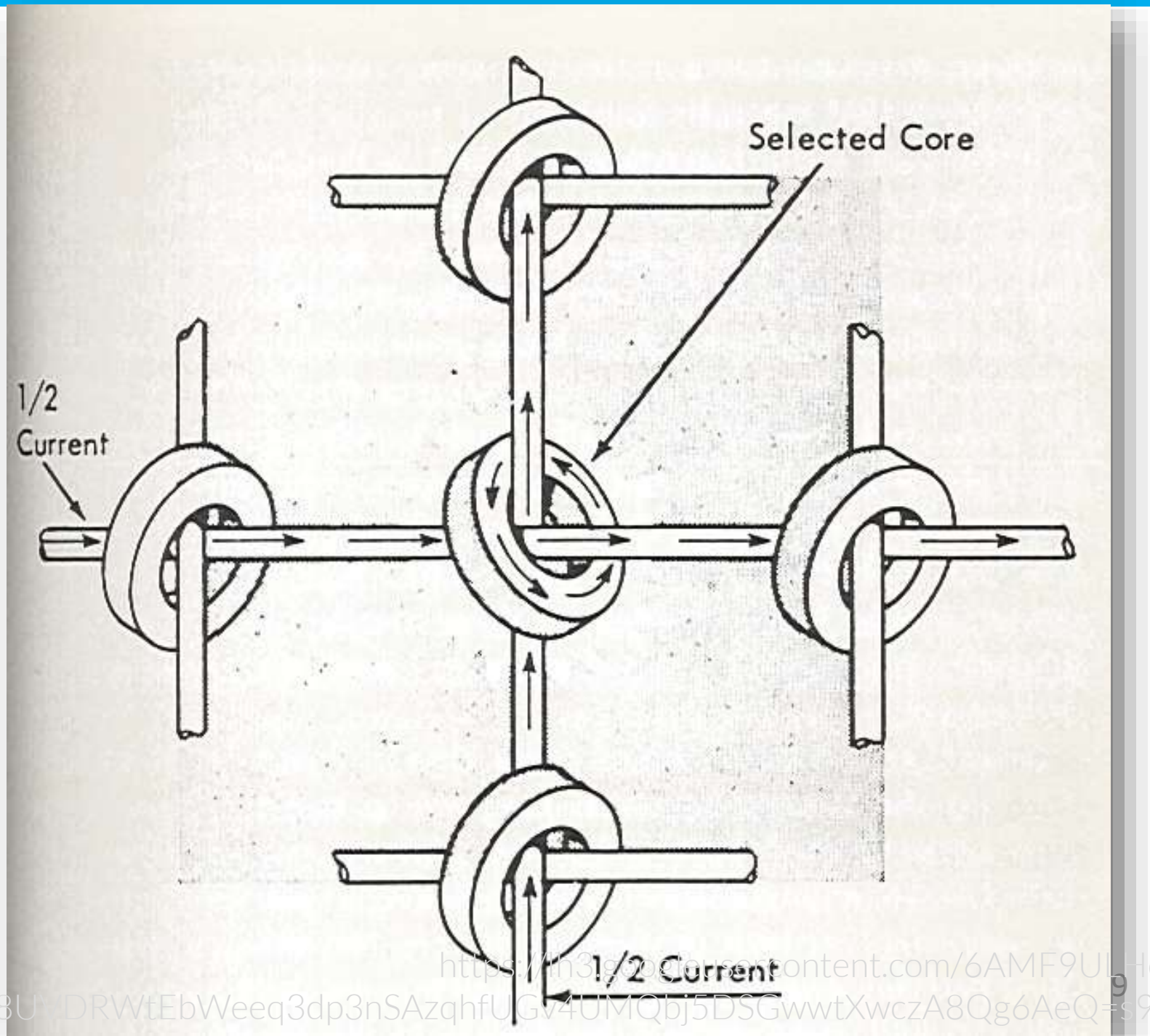
http://www.livestory.com.ua/images/1383361-metropolis_01_hirez.jpg
https://pbs.twimg.com/media/DAmhhBQXoAAxqPA.jpg
http://cityedwire.org/wp-content/uploads/2016/11/on-the-wire.jpg

PRINTERS, TERMINALS AND SCREENS, OH MY!

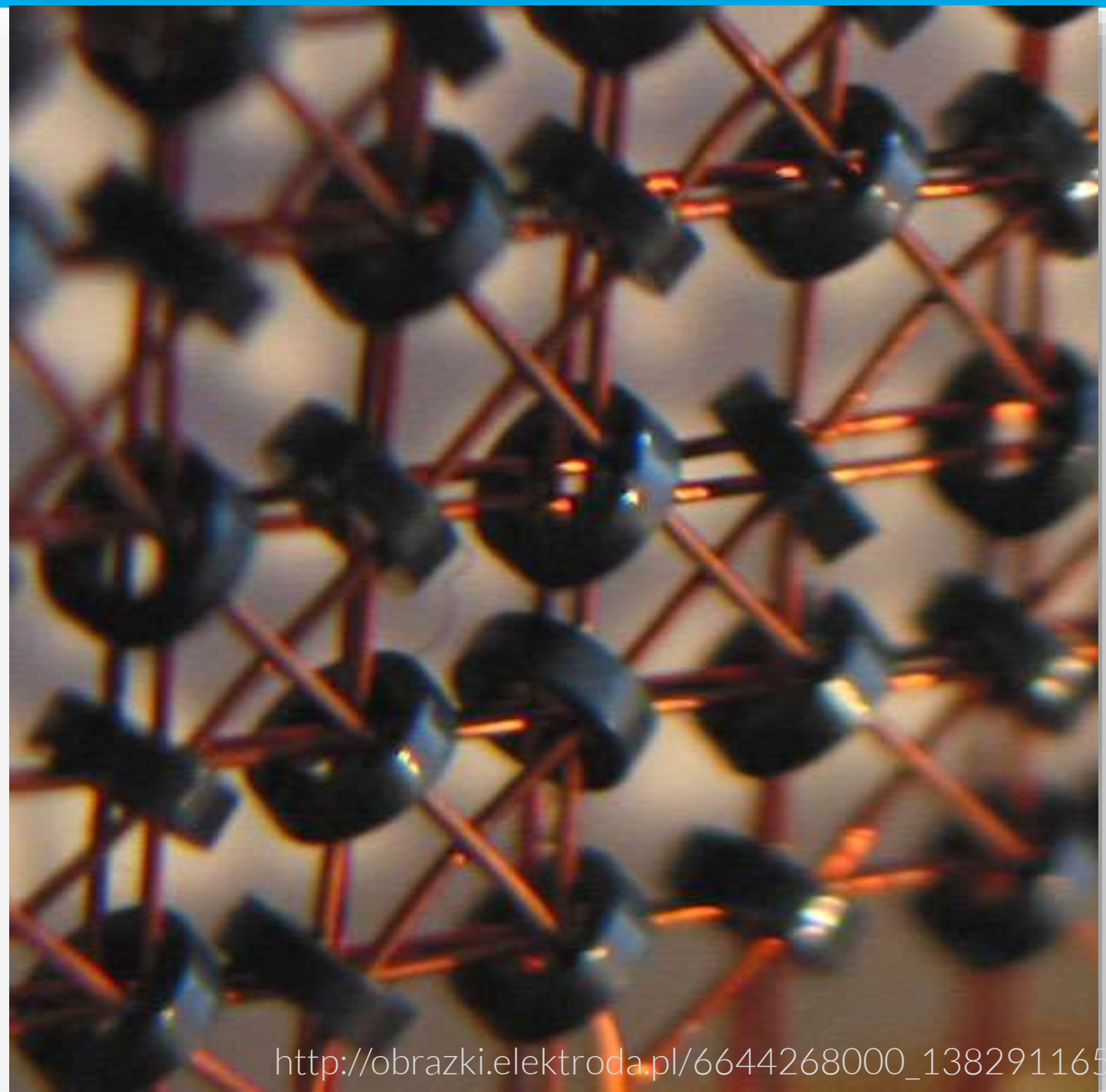
http://hackadaycom.files.wordpress.com/2014/02/adm3a.jpg

MODEMS – THE WORLD OF LOW BANDWIDTH

CURRENT SPIKE DETECTION

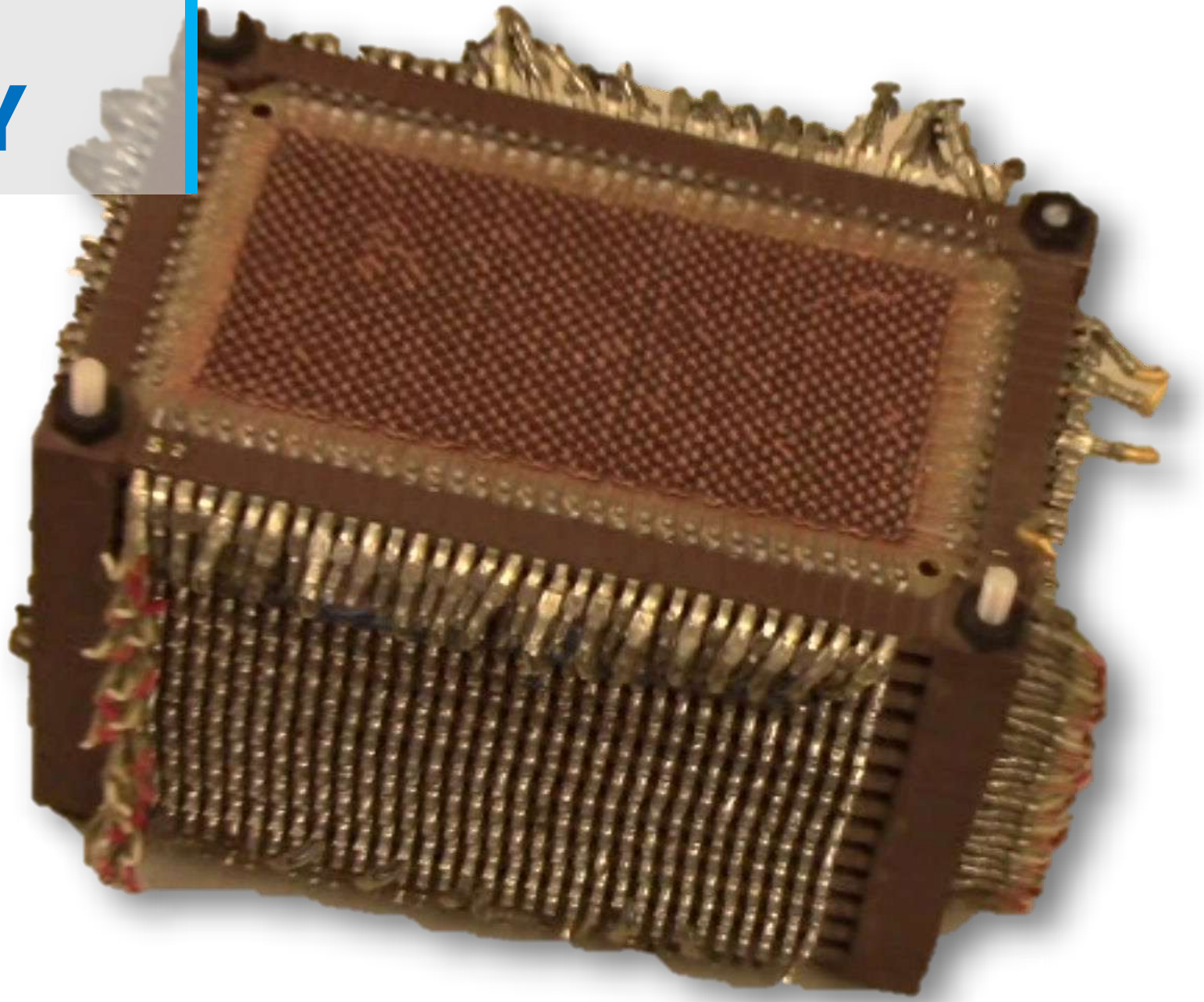


WEAVING FERRITE CORES



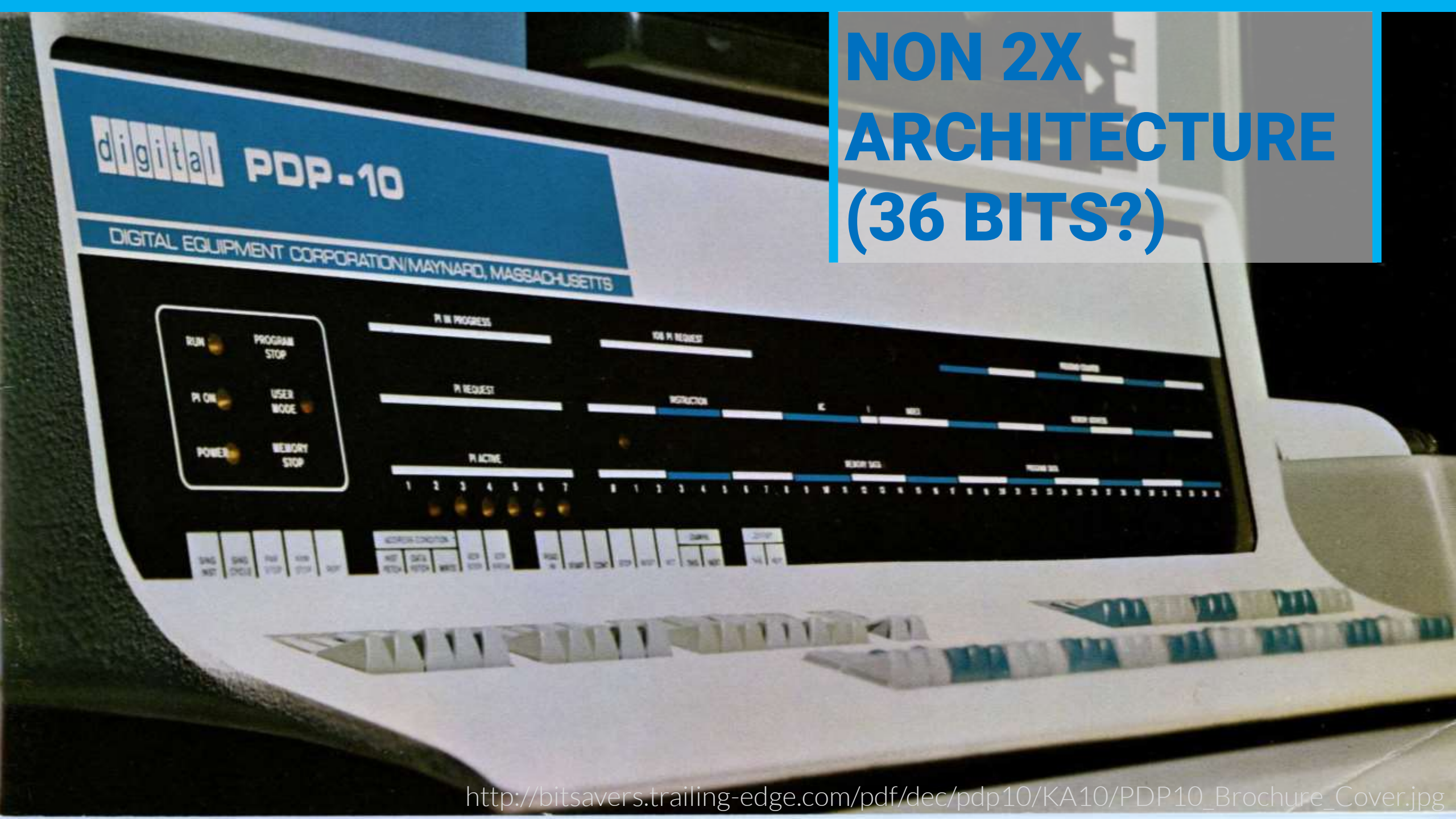
http://obrazki.elektroda.pl/6644268000_1382911653.jpg

CORE MEMORY



https://i.ytimg.com/vi/3rfCDM5olfg/maxresdefault.jpg

NON 2X ARCHITECTURE (36 BITS?)



http://bitsavers.trailing-edge.com/pdf/dec/pdp10/KA10/PDP10_Brochure_Cover.jpg

SERIAL PROTOCOLS

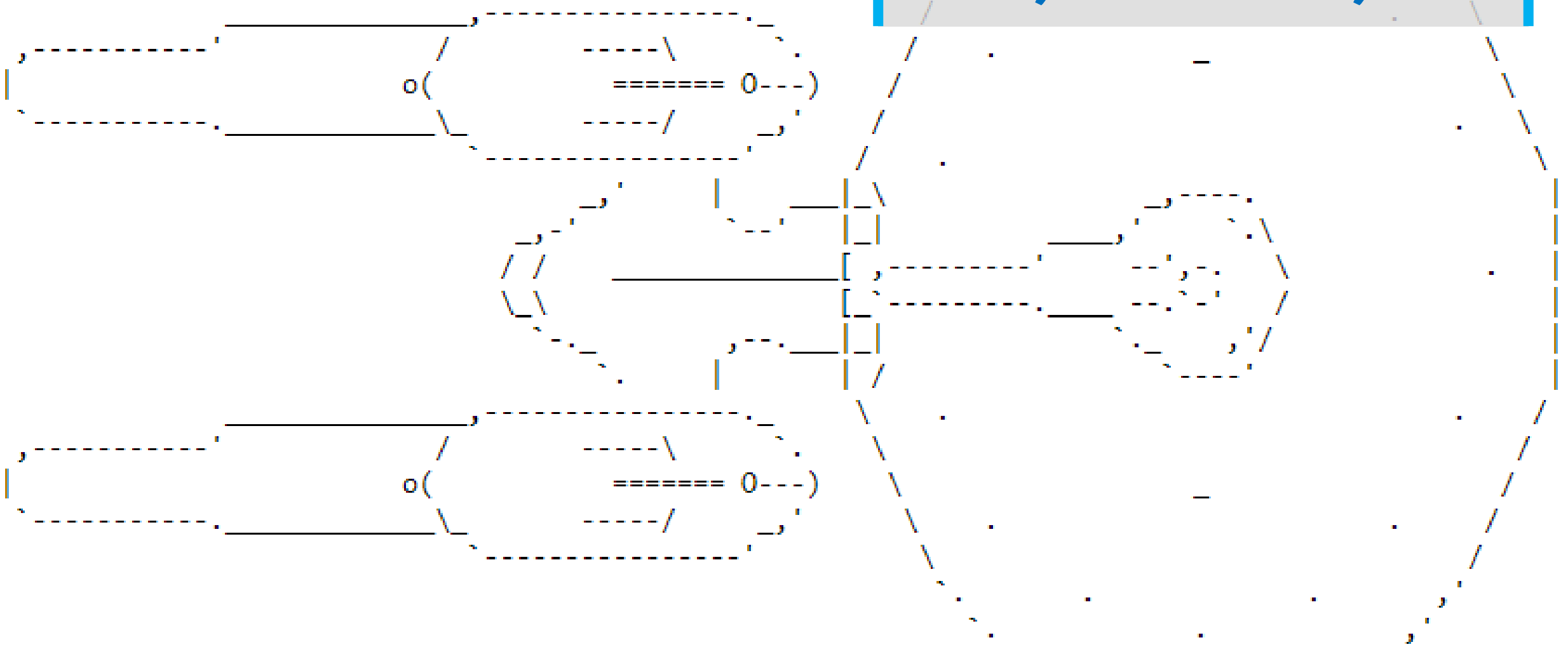
http://www.d-netcable.com/image/data/product/cable/SCNM9FF_1600x1600.jpg

SCREENS? WHERE WE'RE GOING WE DON'T NEED ANY SCREENS

https://i.ytimg.com/vi/DtytP-dA_OM/maxresdefault.jpg


MAIN
PRE INTERNET:
BBS, USENET, IRC
to Pause
ACE) to abort
-O On-Line Help
-T Display System Time
Join Conference(if avail)
Extended Commands Menu
T ransfers
On-line Programs (Doors)
efaults
G -files
* List Available Subs
R emove a Message
P ost a Message
>,+ Advance one Sub #
<,- Retreat one Sub #
N ew Message s
Q N-Scan Current
S can Message Tit
Z Continuous N-S
Goto Sub #
Pres
Electronic Mail
F eedback to Sysop
M ailbox scan
E -Mail a U
K ill E-mail You s
Misc Commands
uto-Message
O ff
our info
U ser List
B BS List
C hat with Sysop
V oting Booth
System I nfo
L ast Callers Today
X Toggle Expert/Novi
http://i.imgur.com/Yj3AnGJ.jpg

PRE INTERNET: BBS, USENET, IRC



https://lh3.googleusercontent.com/USnwb3zBNQg7etw7YgUeKM0EuUUxioloe-JtLy9k7gUu59JCxX1QWenjojZx0PHCq0zV3dg=s85

"YOU ARE IN A MAZE OF TWISTY LITTLE PASSAGES, ALL ALIKE“

```
You are in a splendid chamber thirty feet high.  The walls are frozen rivers
of orange stone.  An awkward canyon and a good passage exit from east and
west sides of the chamber.
>W
At your feet is a small pit breathing traces of white mist.  An east passage
ends here except for a small crack leading on.
Rough stone steps lead down the pit.
>d
You are at one end of a vast hall stretching forward out of sight to the
west.  There are openings to either side.  Nearby, a wide stone staircase
leads downward.  The hall is filled with wisps of white mist swaying to and
fro almost as if alive.  A cold wind blows up the staircase.  There is a
passage at the top of a dome behind you.
Rough stone steps lead up the dome.
>d
You are in the hall of the mountain king, with passages off in all
directions.
```

http://store-images.microsoft.com/image/apps.5188.9007199266436504.cf206bd4-5700-4ba1-ae1d-10a9afa11537.89bc9ce6-f4f6-427f-a859-c72dc7c9cc1a?w=1399&h=787&q=60

TAKEN.
>READ LEAFLET
WELCOME TO ZORK
      ZORK IS A GAME OF ADVENTURE,
DANGER, AND LOW CUNNING. IN IT YOU WILL
EXPLORE SOME OF THE MOST AMAZING
TERRITORY EVER SEEN BY MORTALS.

      NO COMPUTER SHOULD BE WITHOUT ONE!

      THE ORIGINAL ZORK WAS CREATED BY TIM
ANDERSON, MARC BLANK, BRUCE DANIELS, AND
DAVE LEBLING. IT WAS INSPIRED BY THE
ADVENTURE GAME OF CROWTHER AND WOODS.
THIS VERSION WAS CREATED BY MARC BLANK,
DAVE LEBLING, JOEL BEREZ, AND SCOTT
CUTLER.

      (C) COPYRIGHT 1979 & 1980 INFOCOM,
INC. ALL RIGHTS RESERVED.

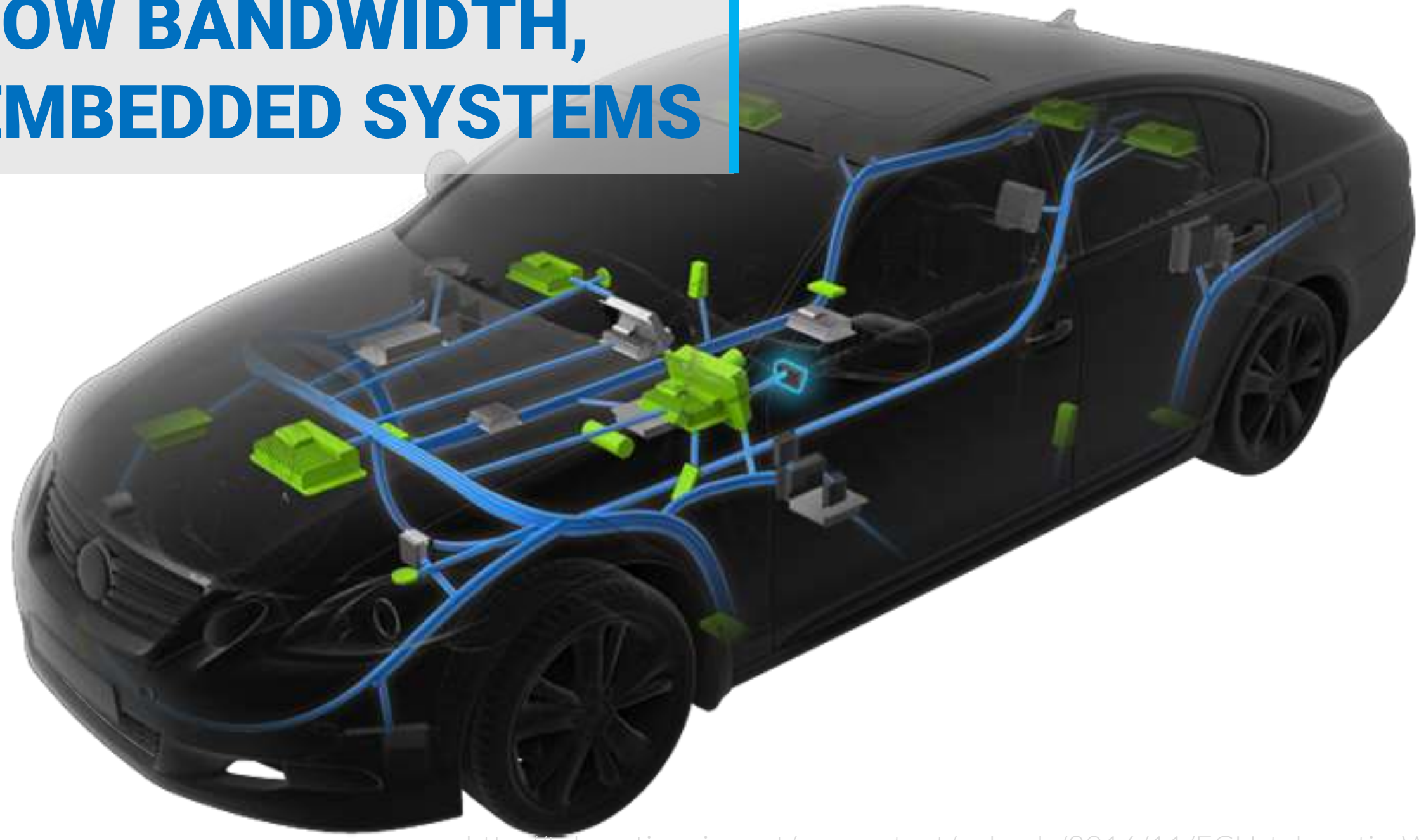
ASCII

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

THAT WAS THE PAST, WHAT ABOUT NOW?

https://i.ytimg.com/vi/BMkoTKnRnJM/maxresdefault.jpg

LOW BANDWIDTH, EMBEDDED SYSTEMS



http://telematicswire.net/wp-content/uploads/2016/11/ECU_telematicsWire.jpg

SERIAL, BANDWIDTH, AND POWER ISSUES

http://www.framboise314.fr/wp-content/uploads/2016/06/PLC-ARDUINO-M-DUINO-58-DIG-1.png

LOW LEVEL IS KEY FOR ANALYSIS

Functions window

Function name	Segm
KeQuerySystemTime	.text
NtQueryInformationFile	.text
NtQueryVolumeInformationFile	.text
NtReadFile	.text
NtWriteFile	.text
NtWaitForSingleObjectEx	.text
NtClose	.text
NtSetInformationFile	.text
NtQueryFullAttributesFile	.text
RtlImageXexHeaderField	.text
NtFreeVirtualMemory	.text
NtFlushBuffersFile	.text
NtAllocateVirtualMemory	.text
ExAllocatePool	.text
KeBugCheckEx	.text
RtlCompareMemoryUlong	.text
NtQueryVirtualMemory	.text
RtlRaiseException	.text
NtCreateEvent	.text
NtSetEvent	.text
NtClearEvent	.text
NtDuplicateObject	.text
NtResumeThread	.text
RtlUnicodeToMultiByteN	.text
NtCancelTimer	.text
NtSetTimerEx	.text
ExTerminateThread	.text
NtCreateTimer	.text
RtlMultiByteToUnicodeN	.text
RtlFreeAnsiString	.text
RtlUnicodeStringToAnsiString	.text
RtlInitUnicodeString	.text

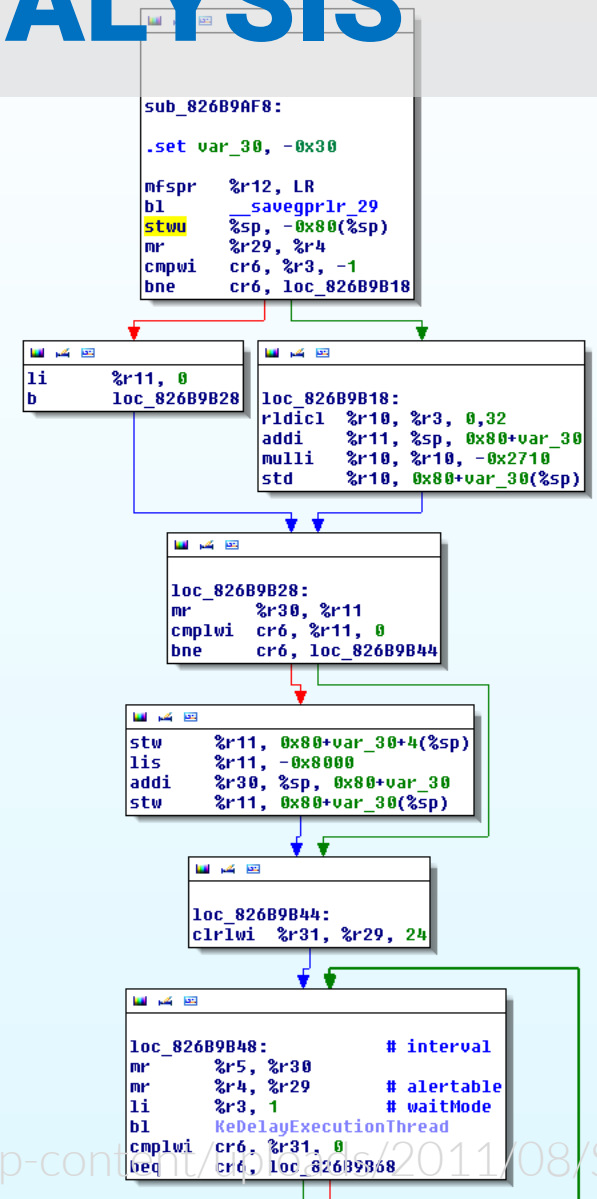
Line 12221 of 12296

Graph overview

IDA View-A, IDA View-B | .text:82392000 | IDA View-A | Structures

IDA View-A

```
.text:826B9AF8
.text:826B9AF8
.text:826B9AF8 sub_826B9AF8:                           # CODE XREF: sub_826B2EA0+10↑p
.text:826B9AF8                                         # sub_826B2ED8+4↑j
.text:826B9AF8
.text:826B9AF8 .set var_30, -0x30
.text:826B9AF8
.text:826B9AF8                mfspr   %r12, LR
.text:826B9AFC                bl      __savegprlr_29
.text:826B9B00                stwu    %sp, -0x80(%sp)
.text:826B9B04                mr      %r29, %r4
.text:826B9B08                cmpwi   cr6, %r3, -1
.text:826B9B0C                bne     cr6, loc_826B9B18
.text:826B9B10                li      %r11, 0
.text:826B9B14                b       loc_826B9B28
.text:826B9B18 # ---------------------------------------------------------------------------
.text:826B9B18
.text:826B9B18 loc_826B9B18:                           # CODE XREF: sub_826B9AF8+14↑j
.text:826B9B18                rldicl  %r10, %r3, 0,32
.text:826B9B1C                addi    %r11, %sp, 0x80+var_30
.text:826B9B20                mulli   %r10, %r10, -0x2710
.text:826B9B24                std     %r10, 0x80+var_30(%sp)
.text:826B9B28
.text:826B9B28 loc_826B9B28:                           # CODE XREF: sub_826B9AF8+1C↑j
.text:826B9B28                mr      %r30, %r11
.text:826B9B2C                cmplwi  cr6, %r11, 0
.text:826B9B30                bne     cr6, loc_826B9B44
.text:826B9B34                stw     %r11, 0x80+var_30+4(%sp)
.text:826B9B38                lis     %r11, -0x8000
.text:826B9B3C                addi    %r30, %sp, 0x80+var_30
.text:826B9B40                stw     %r11, 0x80+var_30(%sp)
.text:826B9B44
.text:826B9B44 loc_826B9B44:                           # CODE XREF: sub_826B9AF8+38↑j
.text:826B9B44                clrlwi  %r31, %r29, 24
.text:826B9B48
.text:826B9B48 loc_826B9B48:                           # CODE XREF: sub_826B9AF8+6C↓j
.text:826B9B48                mr      %r5, %r30       # interval
.text:826B9B4C                mr      %r4, %r29       # alertable
.text:826B9B50                li      %r3, 1          # waitMode
.text:826B9B54                bl      KeDelayExecutionThread
.text:826B9B58                cmplwi  cr6, %r31, 0
.text:826B9B5C                beq     cr6, loc_826B9B68
.text:826B9B60                cmpwi   cr6, %r3, 0x101
.text:826B9B64                beq     cr6, loc_826B9B48
.text:826B9B68
.text:826B9B68 loc_826B9B68:                           # CODE XREF: sub_826B9AF8+64↑j
.text:826B9B68                cmpwi   cr6, %r3, 0xC0
.text:826B9B6C                li      %r3, 0xC0
.text:826B9B70                beq     cr6, loc_826B9B78
.text:826B9B74                li      %r3, 0
.text:826B9B78
.text:826B9B78 loc_826B9B78:                           # CODE XREF: sub_826B9AF8+78↑j
.text:826B9B78                addi    %sp, %sp, 0x80
.text:826B9B7C                b       __restgprlr_29
.text:826B9B7C # End of function sub_826B9AF8
.text:826B9B7C
.text:826B9B80
.text:826B9B80 # =============== S U B R O U T I N E =======================================
.text:826B9B80
.text:826B9B80 # Attributes: thunk
.text:826B9B80
.text:826B9B80 sub_826B9B80:                           # CODE XREF: sub_826B2EE0+1C↑p
.text:826B9B80                                         # sub_826B2F20:loc_826B2F78↑p ...
.text:826B9B80                b       sub_826B8FE0
.text:826B9B80 # End of function sub_826B9B80
```



SMALL DATA • MANY DEVICES = BIG DATA

Example coming up in the next slide!

http://printf.eu/wp-content/uploads/2015/12/big-data.jpg

EVERY BYTE COUNTS

```
struct foo10 {
    char c;
    struct foo10 *p;
    short x;
};

struct foo10 {
    char c;             /* 1 byte */
    char pad1[7];       /* 7 bytes */
    struct foo10 *p;    /* 8 bytes */
    short x;            /* 2 bytes */
    char pad2[6];       /* 6 bytes */
};

struct foo11 {
    struct foo11 *p;    /* 8 bytes */
    short x;            /* 2 bytes */
    char c;             /* 1 bytes */
    char pad[5];        /* 5 bytes */
};
```


http://hackadaycom.files.wordpress.com/2014/02/adm3a.jpg

WHAT MAKES HACKERS, HACKERS?

RESPECT YOUR ELDERS,

http://3.bp.blogspot.com/-RaQd_ZWduzU/TrV78AF8ChI/AAAAAAAAAIOU/0VyWIaD_ZQU/s1600/Statler+and+Waldorf.jpg

~~RESPECT~~ LEARN FROM YOUR ELDERS, THEY KNOW S@!T

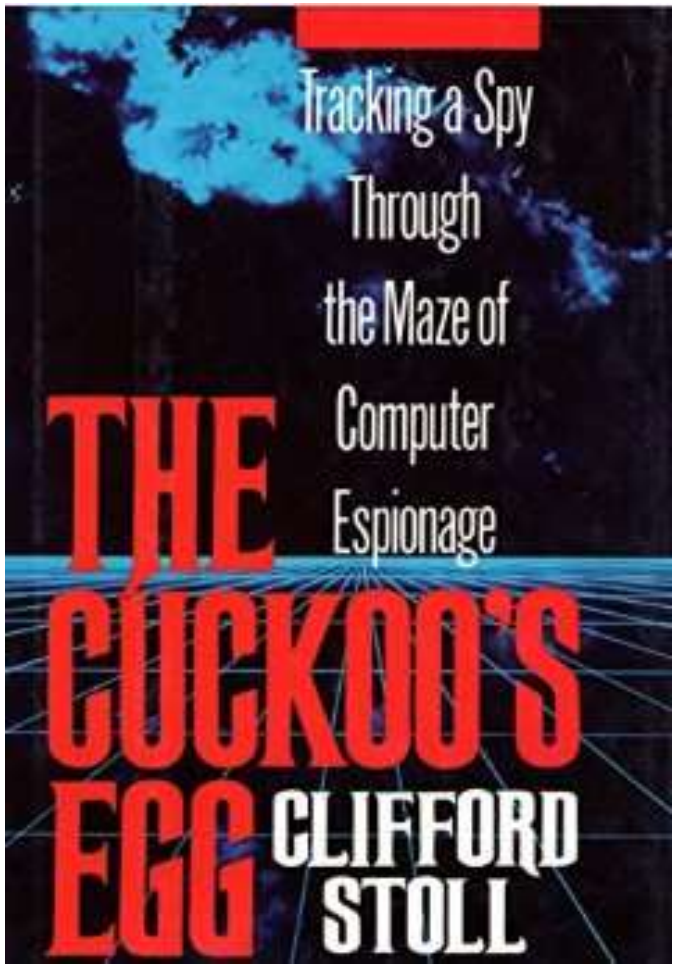
http://3.bp.blogspot.com/-RaQd_ZWduzU/TrV78AF8ChI/AAAAf.jpg

WE ARE NOT ALONE

https://upload.wikimedia.org/wikipedia/commons/4/41/Solder_workshop_at_FIXME_Hackerspace%2C_Renens%2C_Lausanne_%282015-05-23_06.25.46_by_Mitch_Altman%29.jpg

CHECK THESE OUT

- http://www.catb.org/esr/faqs/things-every-hacker-once-knew/
- The Cuckoo's egg, Clifford Stoll, 1989
  - Highly recommended!
- "Things Every Hacker Once Knew"
  - Eric S. Raymond
  - http://www.catb.org/esr/faqs/things-every-hacker-once-knew/

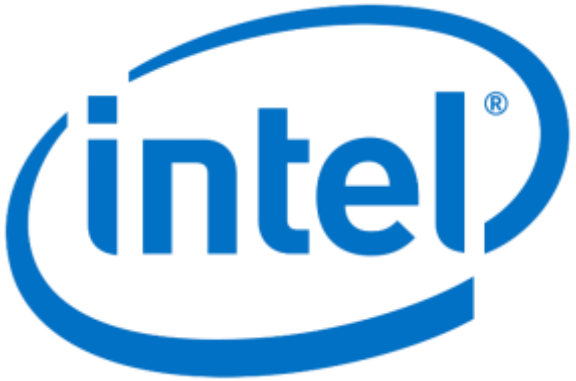


Questions? @barnhartguy, barnhart.guy [at] gmail.com, http://productsecurity.info

https://kbimages1-a.akamaihd.net/3741ee80-ba07-43fe-98a3-89000670bd0f/1200/1200/False/cuckoo-s-egg.jpg

SELF PROMOTION SLIDE

- We are hiring!
  - Haifa
- If you like reverse engineering,
- Like poking around embedded systems, CPUs, Drones, Automotive Computers,
- Talk to me!

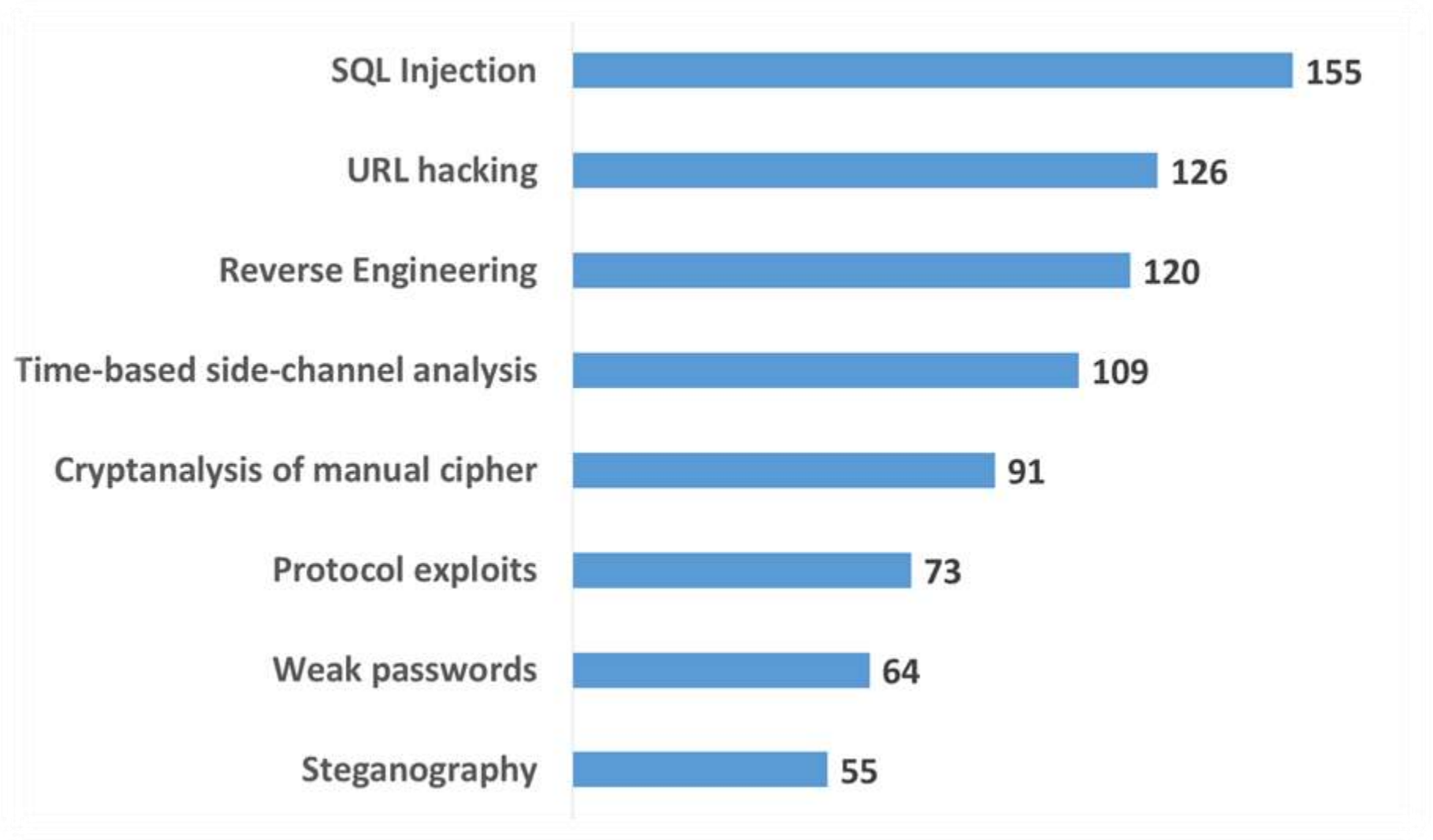


Questions? @barnhartguy, barnhart.guy [at] gmail.com, http://productsecurity.info

ONE LAST THING

Questions? @barnhartguy, barnhart.guy [at] gmail.com, http://productsecurity.info

YOU ARE NOT ALONE



Questions? @barnhartguy, barnhart.guy [at] gmail.com, http://productsecurity.info

CREDITS!

Winners to be announced later today

Thank you for all your feedback! (really)

The website is written in Python 3.6, Flask and Dockerized on EC2

Originally developed at Cisco (2012) by Jon, Michal, Harel, Ofer, Orit and Myself

Questions? @barnhartguy, barnhart.guy [at] gmail.com, http://productsecurity.info