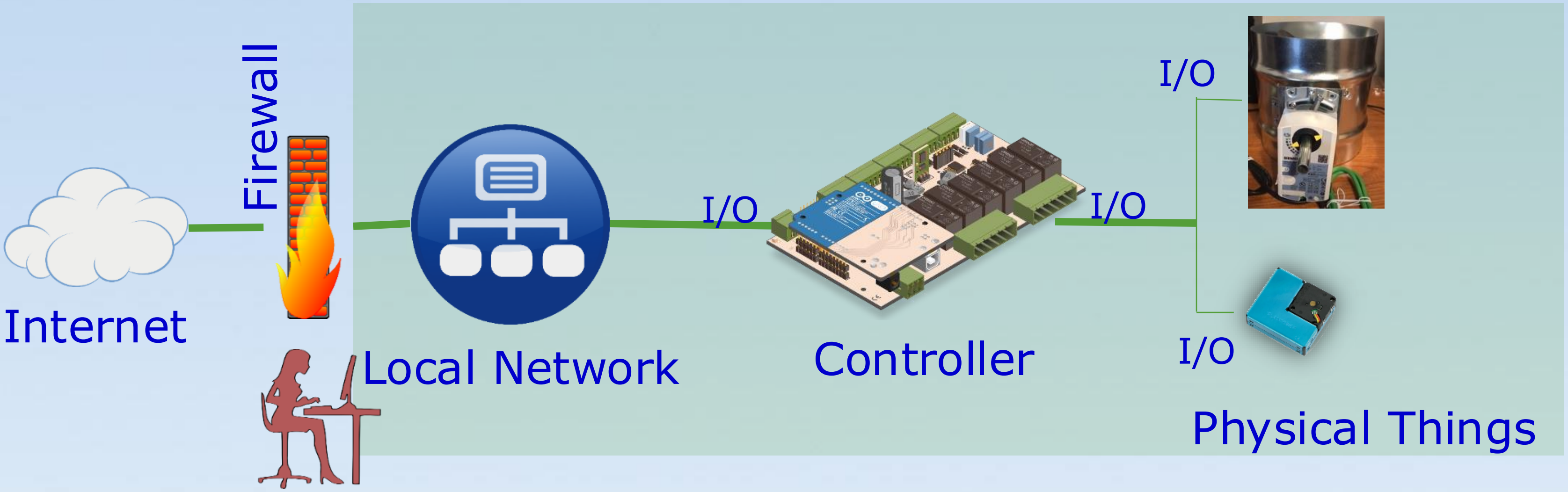
A View of IoT and Emerging Topics

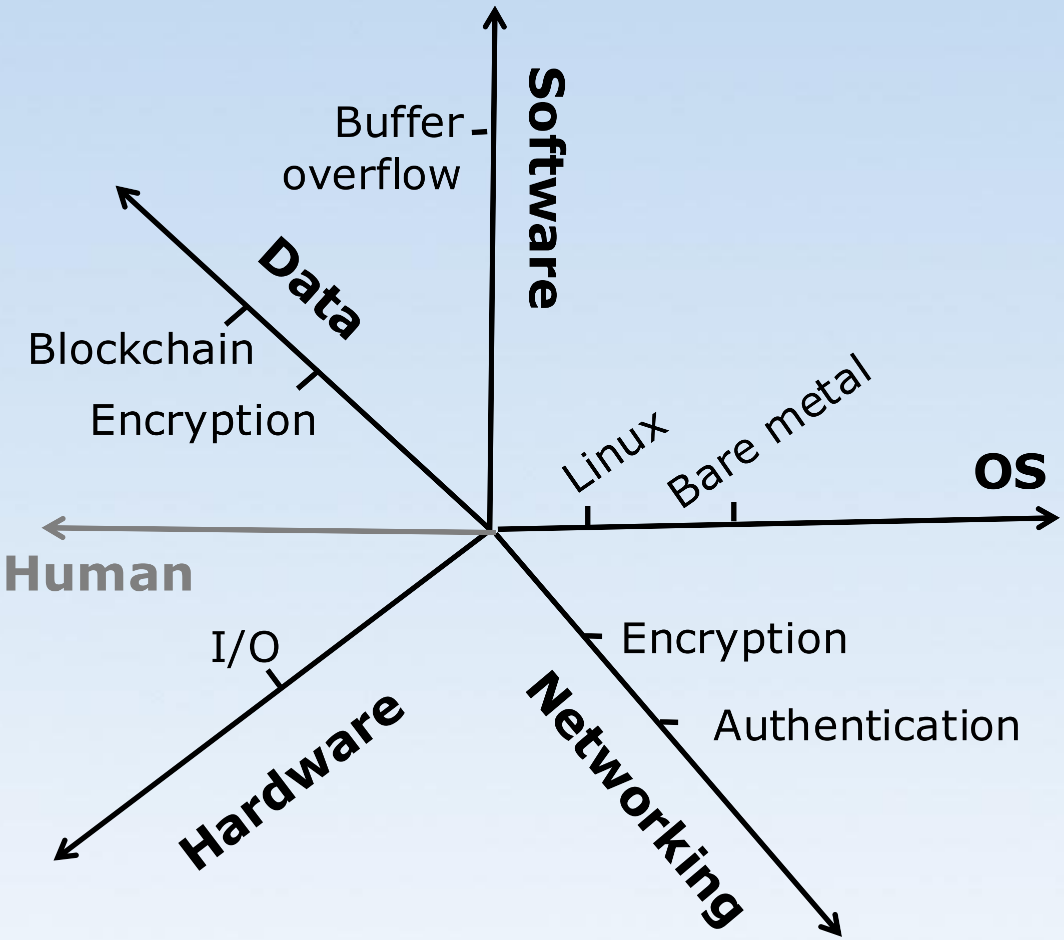
Xinwen Fu
Professor
School of Computer & Information Sciences
University of Massachusetts Lowell

Unified View of IoT and CPS



- Similar in *networking* architecture
  - Communication modules to *things* for networking
- Difference in applications
  - Hardware, OS/Firmware, Software, Networking, Data

Risk Analysis Framework



Misconception

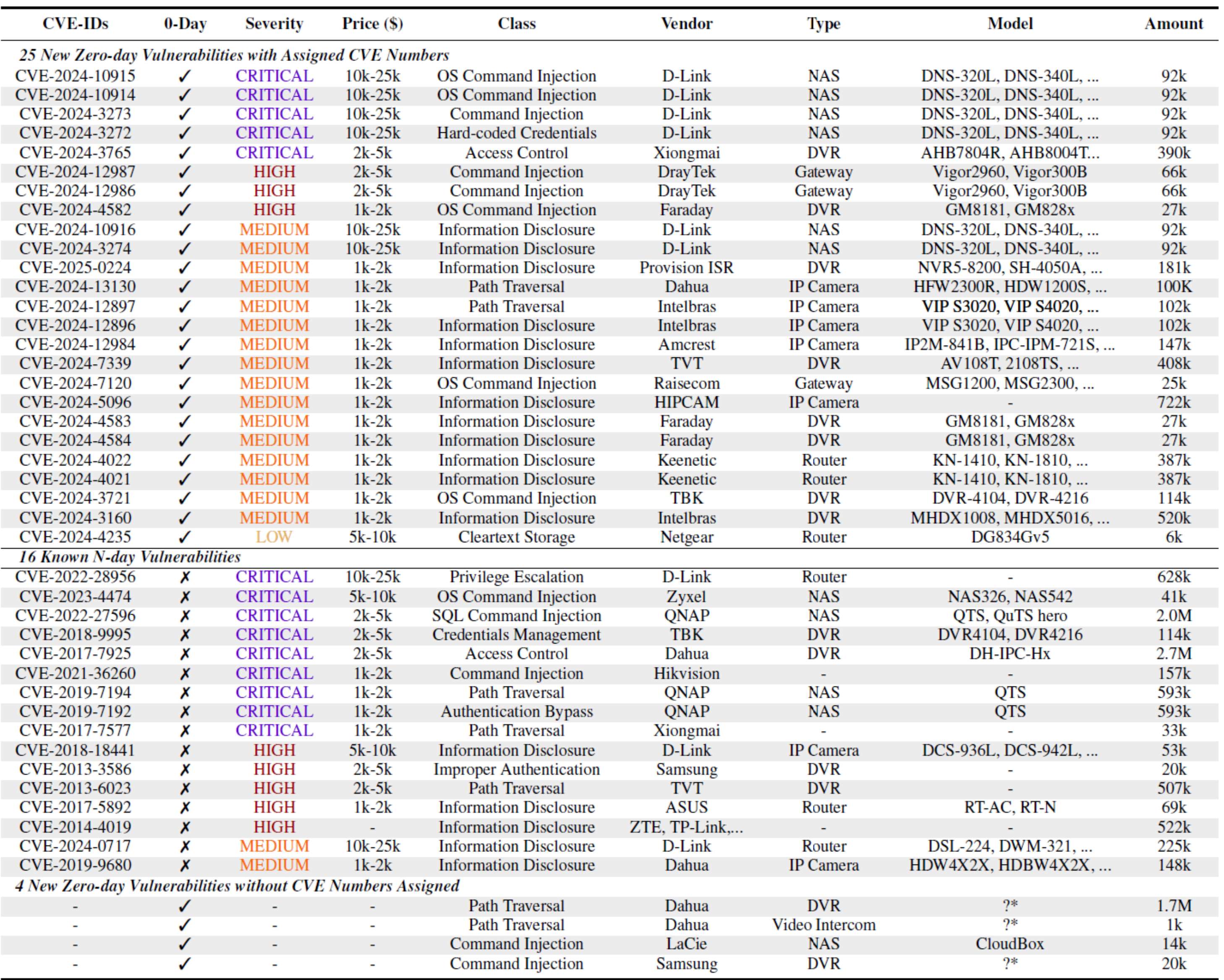
IoT security and privacy issues are caused by expensive secure hardware

Hardware and Costs Causing Security Problems?

- Modern security chips can be cheap
  - $0.55 Microchip ATECC608A crypto coprocessor: AES, ECC, HMAC, SHA-256, and RNG; Secure key storage
- We find: most of time design and implementation is the culprit

Discovering Attacks against IoT on Tor

45 attacks, 29 zero-day discovered through LLM



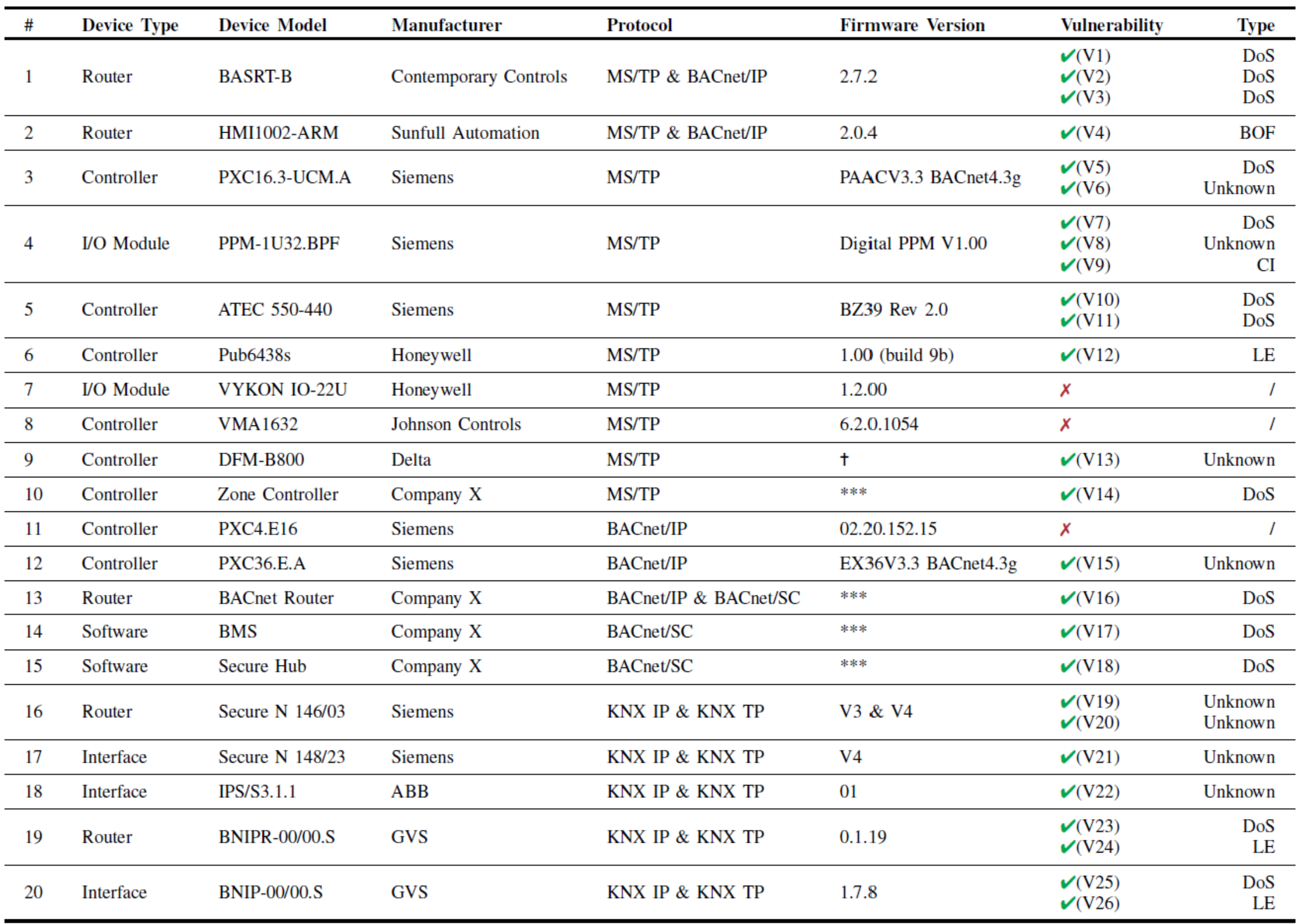
CVE-IDs	0-Day	Severity	Price ($)	Class	Vendor	Type	Model	Amount
25 New Zero-day Vulnerabilities with Assigned CVE Numbers								
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision ISR	DVR	NVR5-8200, SH-4050A, ...	181k
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua	IP Camera	HFW2300R, HDW1200S, ...	100K
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras	IP Camera	**VIP S3020, VIP S4020, ...**	102k
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	VIP S3020, VIP S4020, ...	102k
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	408k
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	25k
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	722k
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k
16 Known N-day Vulnerabilities								
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Hikvision	-	-	157k
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal	QNAP	NAS	QTS	593k
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass	QNAP	NAS	QTS	593k
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal	Xiongmai	-	-	33k
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure	D-Link	IP Camera	DCS-936L, DCS-942L, ...	53k
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication	Samsung	DVR	-	20k
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k
4 New Zero-day Vulnerabilities without CVE Numbers Assigned								
-	✓	-	-	Path Traversal	Dahua	DVR	?*	1.7M
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?*	1k
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k
-	✓	-	-	Command Injection	Samsung	DVR	?*	20k

USENIX Security’25

Discovering Smart Building Protocol BACnet Vulnerabilities

15 BACnet and 5 KNX devices & software through fuzzing and LLM

NDSS’26



#	Device Type	Device Model	Manufacturer	Protocol	Firmware Version	Vulnerability	Type
1	Router	BASRT-B	Contemporary Controls	MS/TP & BACnet/IP	2.7.2	✔(V1) ✔(V2) ✔(V3)	DoS DoS DoS
2	Router	HMI1002-ARM	Sunfull Automation	MS/TP & BACnet/IP	2.0.4	✔(V4)	BOF
3	Controller	PXC16.3-UCM.A	Siemens	MS/TP	PAACV3.3 BACnet4.3g	✔(V5) ✔(V6)	DoS Unknown
4	I/O Module	PPM-1U32.BPF	Siemens	MS/TP	Digital PPM V1.00	✔(V7) ✔(V8) ✔(V9)	DoS Unknown CI
5	Controller	ATEC 550-440	Siemens	MS/TP	BZ39 Rev 2.0	✔(V10) ✔(V11)	DoS DoS
6	Controller	Pub6438s	Honeywell	MS/TP	1.00 (build 9b)	✔(V12)	LE
7	I/O Module	VYKON IO-22U	Honeywell	MS/TP	1.2.00	✗	/
8	Controller	VMA1632	Johnson Controls	MS/TP	6.2.0.1054	✗	/
9	Controller	DFM-B800	Delta	MS/TP	†	✔(V13)	Unknown
10	Controller	Zone Controller	Company X	MS/TP	***	✔(V14)	DoS
11	Controller	PXC4.E16	Siemens	BACnet/IP	02.20.152.15	✗	/
12	Controller	PXC36.E.A	Siemens	BACnet/IP	EX36V3.3 BACnet4.3g	✔(V15)	Unknown
13	Router	BACnet Router	Company X	BACnet/IP & BACnet/SC	***	✔(V16)	DoS
14	Software	BMS	Company X	BACnet/SC	***	✔(V17)	DoS
15	Software	Secure Hub	Company X	BACnet/SC	***	✔(V18)	DoS
16	Router	Secure N 146/03	Siemens	KNX IP & KNX TP	V3 & V4	✔(V19) ✔(V20)	Unknown Unknown
17	Interface	Secure N 148/23	Siemens	KNX IP & KNX TP	V4	✔(V21)	Unknown
18	Interface	IPS/S3.1.1	ABB	KNX IP & KNX TP	01	✔(V22)	Unknown
19	Router	BNIPR-00/00.S	GVS	KNX IP & KNX TP	0.1.19	✔(V23) ✔(V24)	DoS LE
20	Interface	BNIP-00/00.S	GVS	KNX IP & KNX TP	1.7.8	✔(V25) ✔(V26)	DoS LE

Thoughts

- LLM and AI can play a big role to automate vulnerability discovery
- How much data to feed into the LLM and AI for discovery vs privacy?
- LLM and AI for *real-time* discovery?
- General prompt engineering theories for security?