Tempest

ACADEMY

Conference

2023

DDoS em tempos (pós) IoT

João Gondim

Depto. Ciência da Computação - CIC
UnB

Tempest

ACADEMY

Conference

01 Apresentação

02 O Cenário e IoT

03 DDoS: tendências e perspectivas

04 Comentários finais

Apresentação

Principais frentes de pesquisa

Tempest
:ACADEMY:
Conference

Detecção de incidentes por anomalia

Dinâmica de ataques volumétricos incapacitantes

Atribuição de origem

Orquestração cibernética: arquiteturas de C&C

Cyber Threat Hunting/Intelligence

Parcerias/colaborações relevantes

Tempest
:ACADEMY:
Conference

Marcelo Marotta - CIC/UnB
Luis Paulo Faina Garcia - CIC/UnB
Robson Albuquerque - PPEE/ENE/UnB
André Gregio – DI/UFPr, Brasil

Luis Javier García Villalba - Univ Complutense de Madrid, Espanha
Matt Bishop – UC at Davies, USA
Luiz da Silva – Virginia Tech, USA
Jens Pedersen – Aalborg Unviversity, Denmark
Diego Aranha – Aarhus University, Denmark
Bernardo David – ITU Copenhagen, Denmark
Rafael Dowsley – Monash University, Australia
Cristoffer Leite – Eindhoven Technical University, Holland

Nano CV

Tempest
[ACADEMY]
Conference

1980-1984 – Engenharia Elétrica, habilitação Eletrônica, UFPE (tenho CREA)

1986-1987 – MSc Computer Science, Imperial College, University of London

1987-1992 - PhD Computer Science, Imperial College, University of London (incompleto)

1994- ? – Professor Depto. de Ciência da Computação, CIC/UnB

2012-2017- PhD Engenharia Elétrica UnB (fiz pelo dinheiro)

+30 anos de experiência em Redes de Computadores

+25 anos de experiência em [Net|Info|Cyber] Security, incluindo projetos “no mundo real” – (não só papel e papers)

Disclaimer

Tempest
[ACADEMY]
Conference

As afirmações aqui expressas são baseadas na minha experiência sendo de minha responsabilidade.

Minhas opiniões não refletem de forma alguma as de meu empregador.

As informações sobre vulnerabilidades e ataques são aqui apresentadas para fins acadêmicos com a finalidade de avançar na segurança e vêm de experimentos e fontes abertas.

Informações específicas sobre vulnerabilidades e ataques foram coletadas para fins puramente didáticos, em ambiente controlado e sob consentimento institucional.

Disclaimer (alt)

Tempest
[ACADEMY]
Conference

I´m a nice guy

Não acredito em “gedanken experimentzen” para segurança.

Nem acredito no “karate kid” approach

Don´t try this at home!

Cenário

Tecnologias emergentes/disruptivas

Tempest
:ACADEMY:
Conference

Cloud Computing

IoT

5G

- Infraestruturas críticas:
  - SCADA/ICS
- IA
  - ML/DL
  - Generativa
    - Adversarial

IoT

Internet of Things

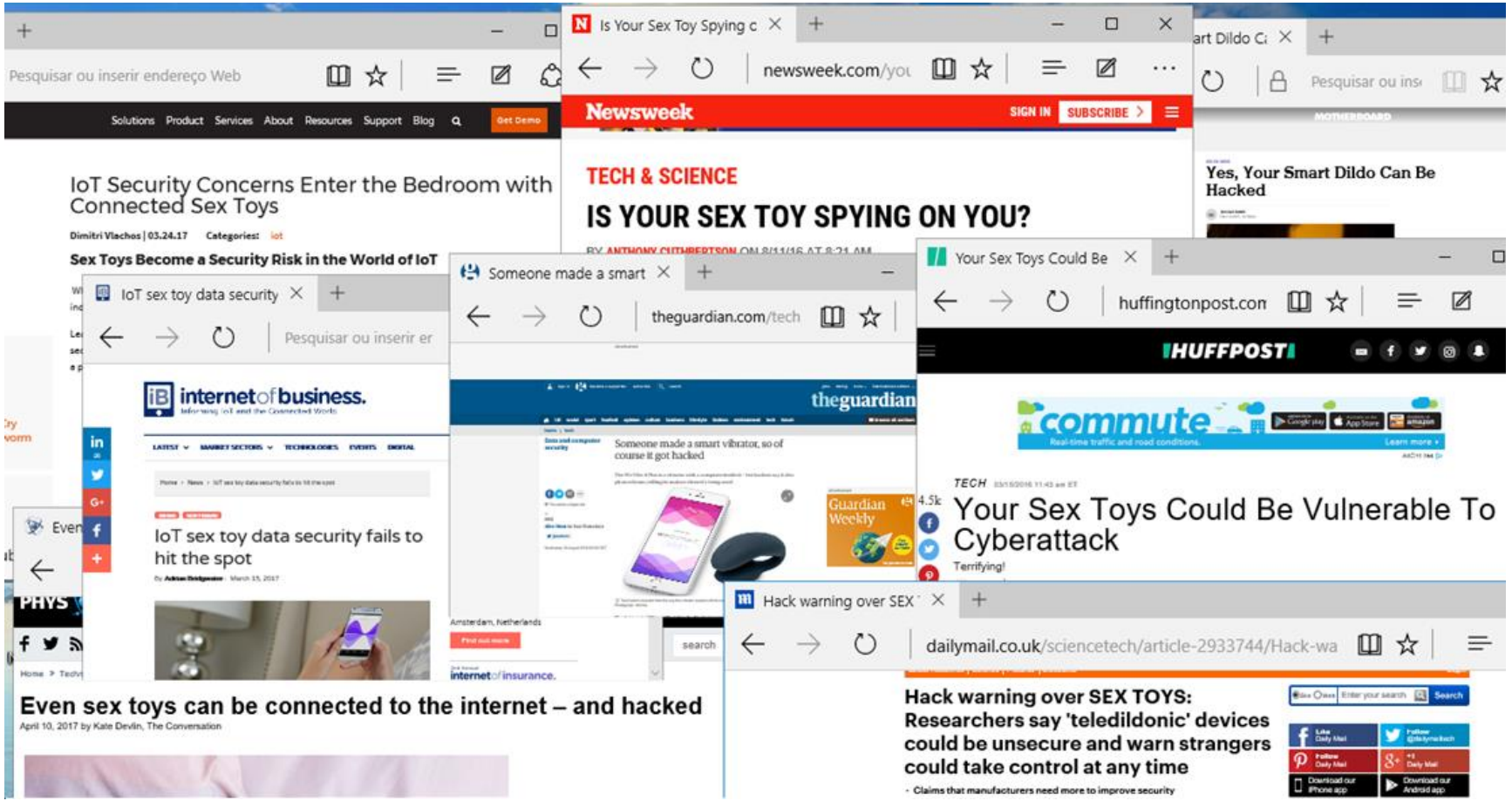
Quais são essas coisas da Internet das Coisas?

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

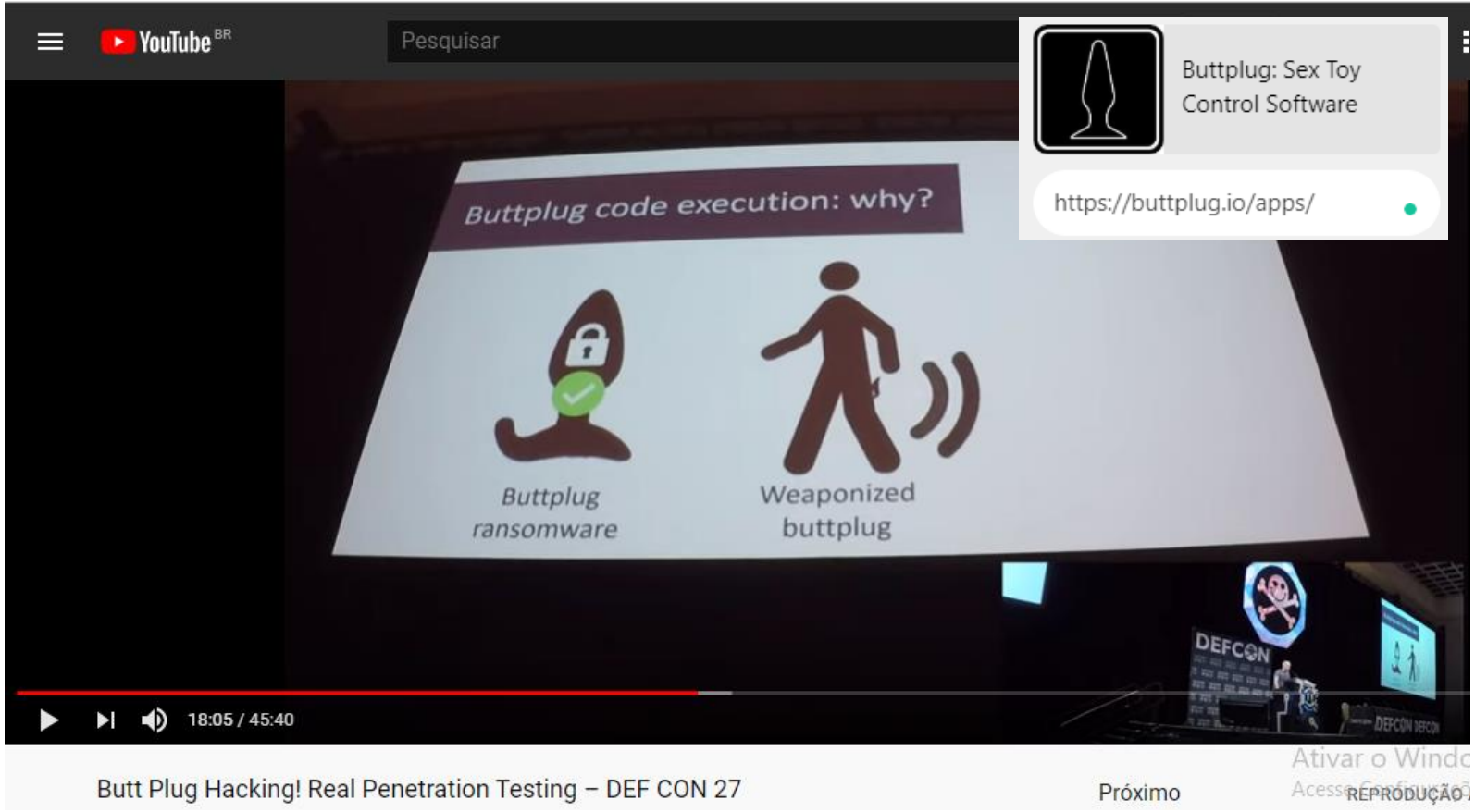
Sunday, April 15, 2018 Wang Wei

Share 8.67k Share Tweet Share

Qualquer coisa?



Qualquer coisa mesmo?



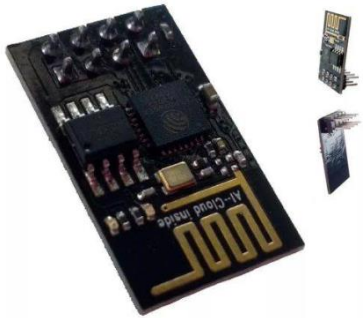
IoT

Dispositivos

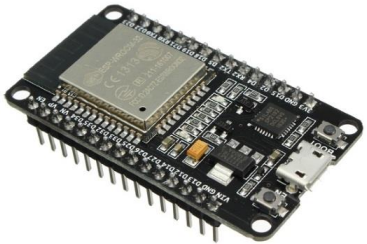
- Gadgets
- Consumer electronics
- Mobile
- Sensors
- SCADA/ICS hardware

- Baixo poder computacional
- Pequeno armazenamento
- Conectividade limitada
- Baixo consumo de energia
- Restrições de implementação
- Foco em funcionalidades
- Segurança (?)

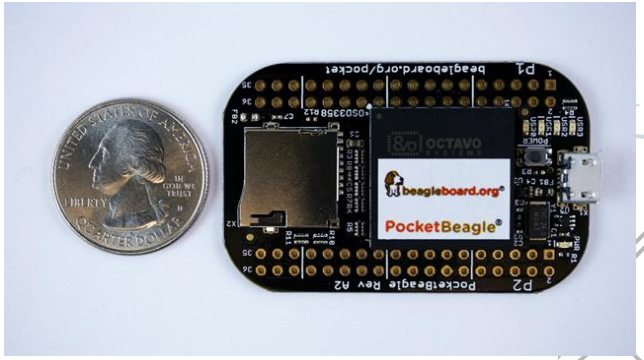
IoT Hardware

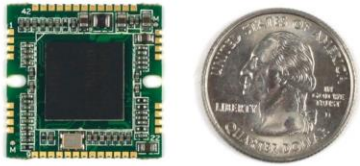


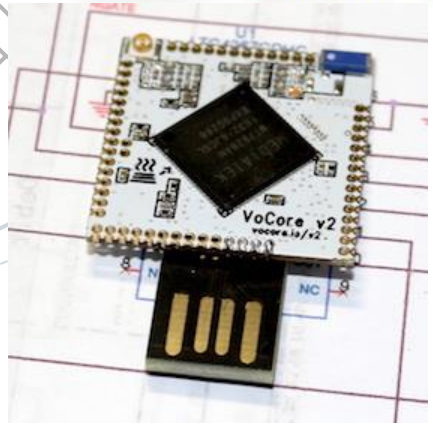
ESP-8266



ESP-32







Kit Arduino Uno R3 Completo...

Arduino Uno Rev3 R3...

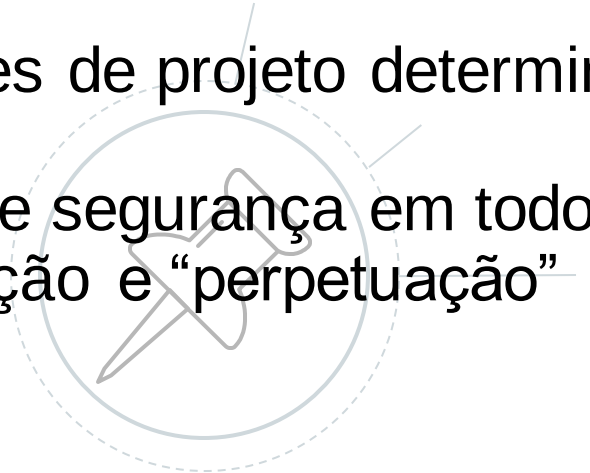
Kit Arduino Start

Placa Raspberry Pi 3 Modelo B

Raspberry Pi 3 - Modelo B

Dispositivos

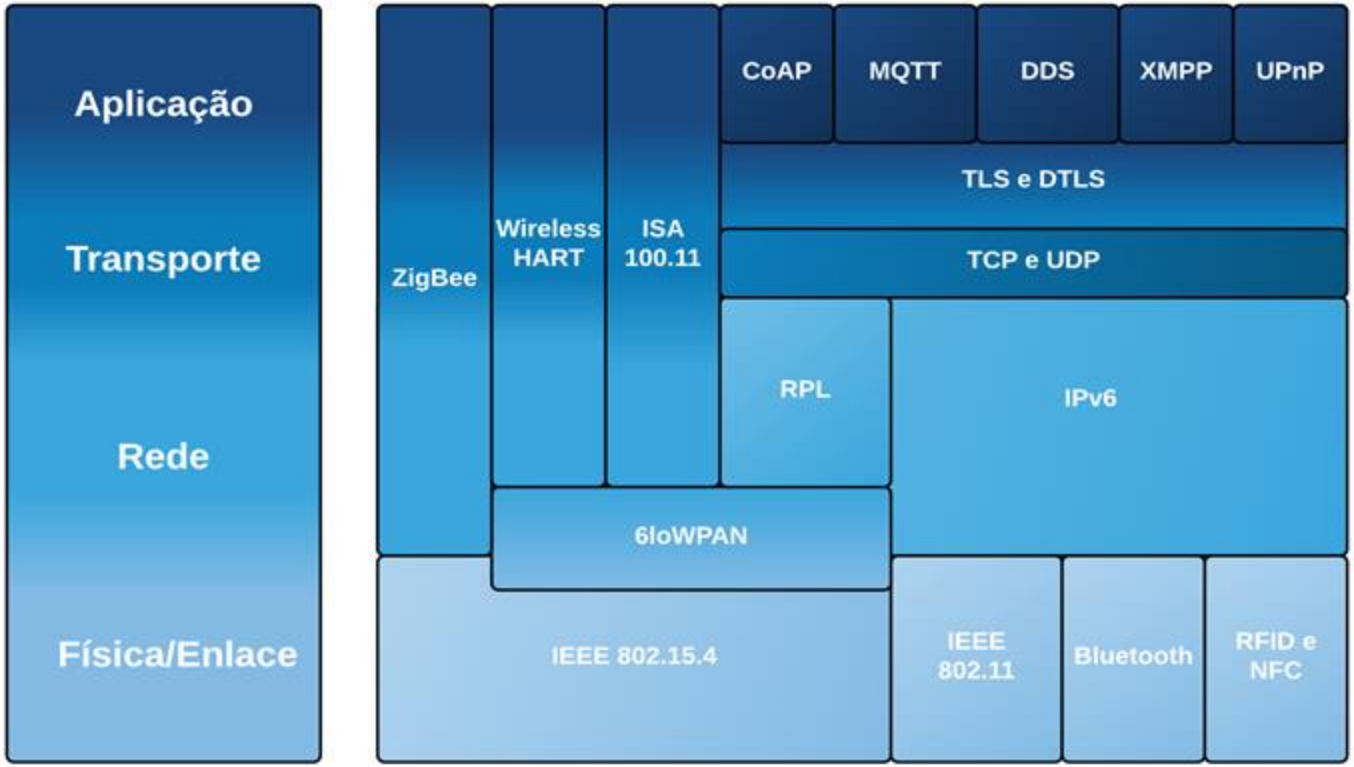
- Descisões de projeto determinadas por custo
- Falhas de segurança em todos os níveis
- Propagação e “perpetuação”



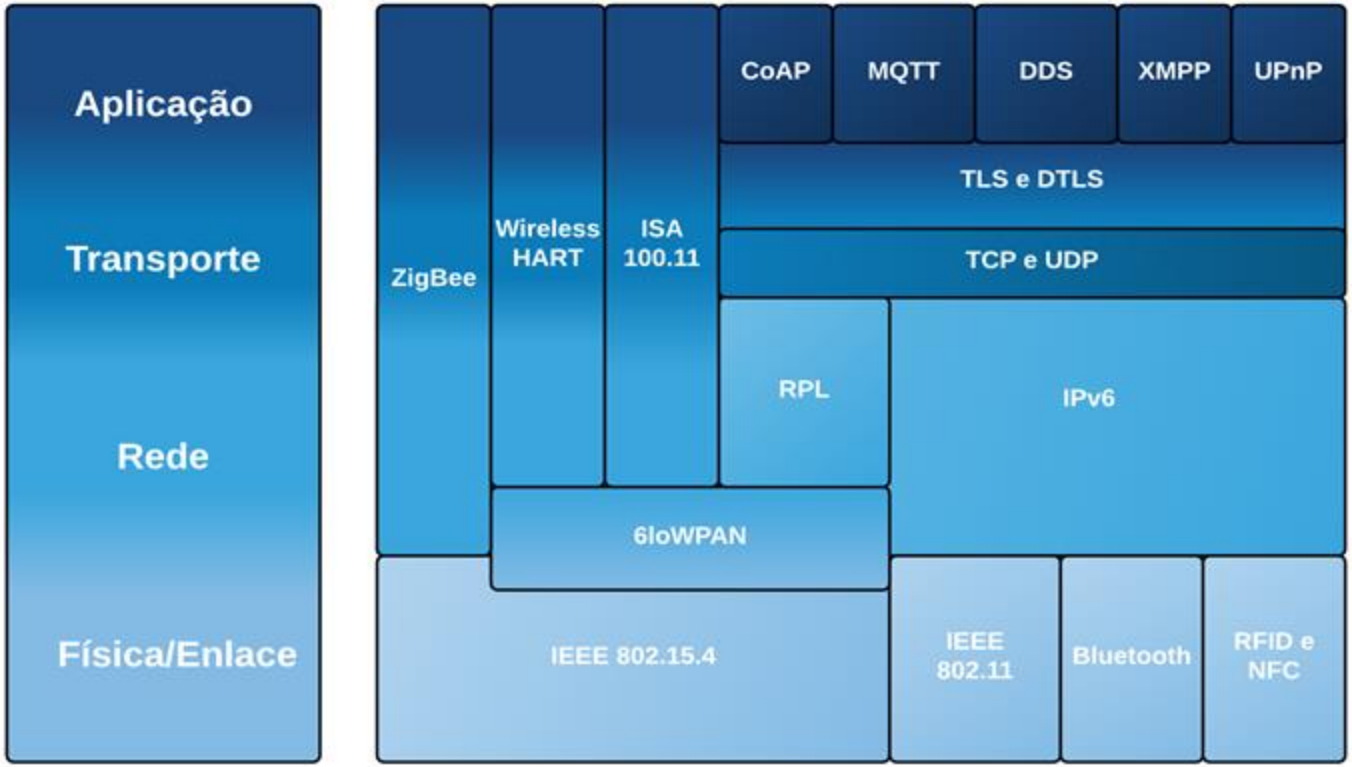
- Security issues em várias camadas:
- Chipsets
- Módulos
- SDKs, APIs, libs
- RTEs e OSs

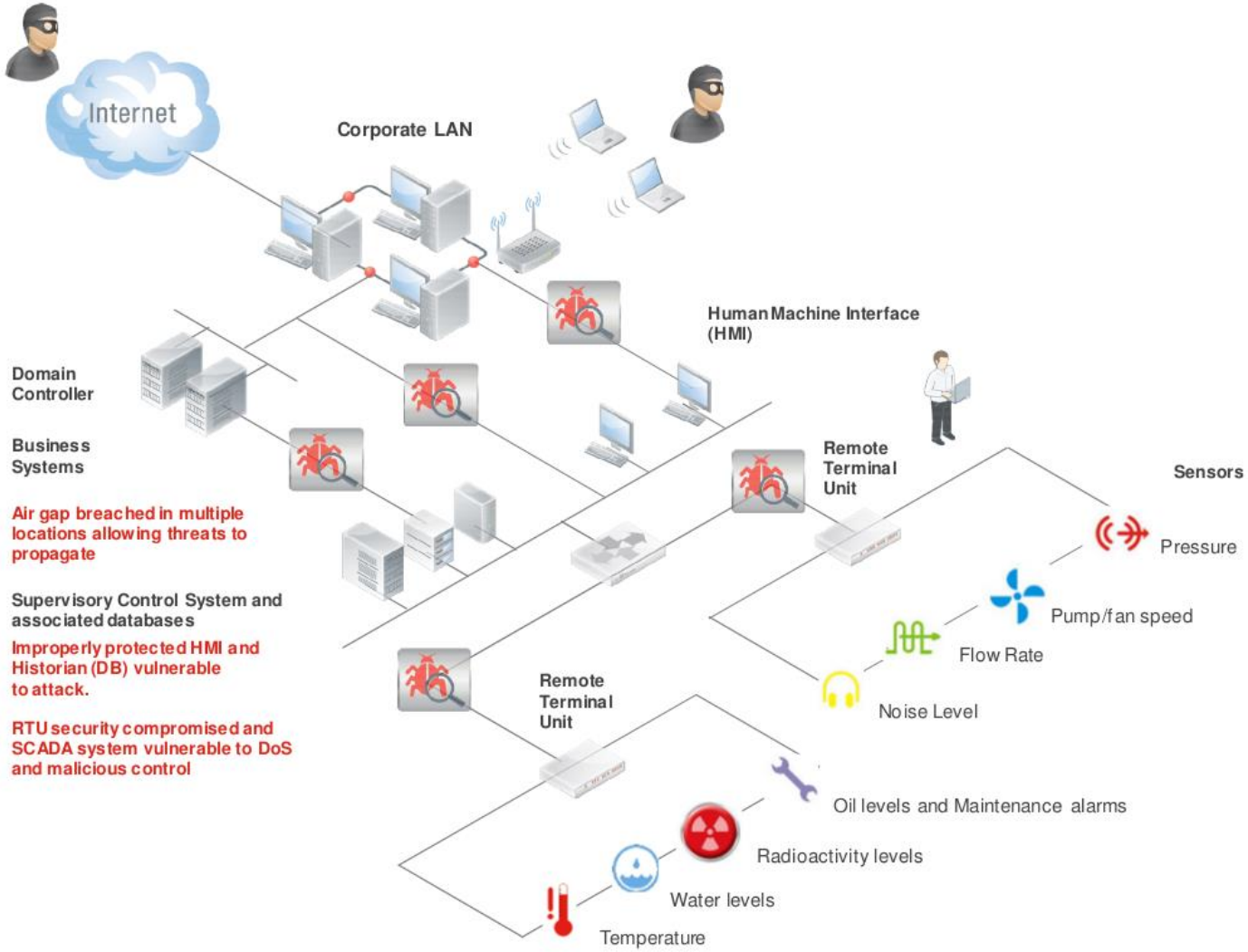
- Se possível:
- Auditoria de código
- Run you own build
- Abordagem dual

Protocolos usados em IoT:



Protocolos usados em IoT:
TODOS têm “security issues”



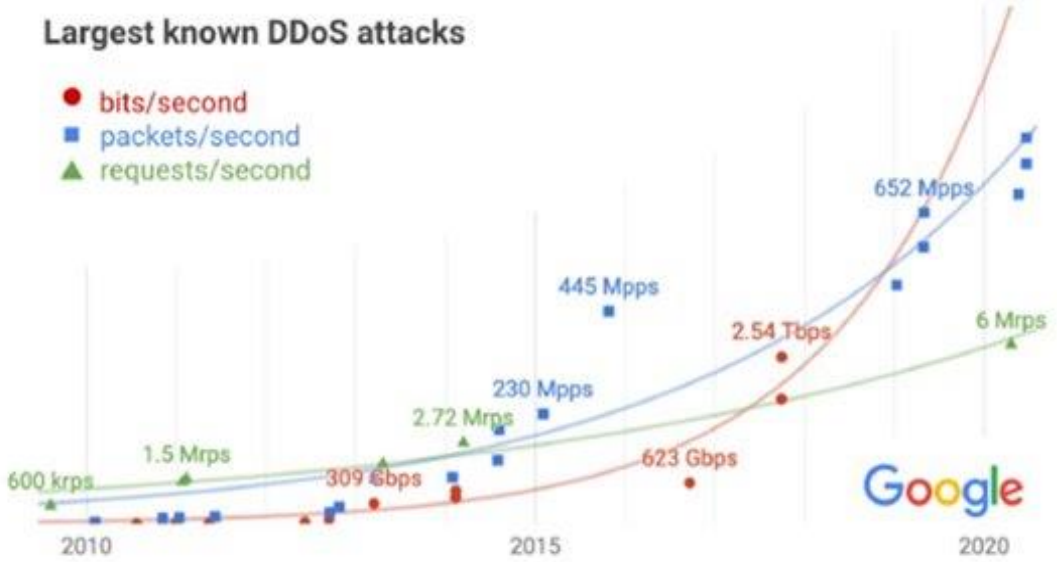

Internet
Corporate LAN
Human Machine Interface (HMI)
Domain Controller
Business Systems
Air gap breached in multiple locations allowing threats to propagate
Supervisory Control System and associated databases
Improperly protected HMI and Historian (DB) vulnerable to attack.
RTU security compromised and SCADA system vulnerable to DoS and malicious control
Remote Terminal Unit
Sensors
Pressure
Pump/fan speed
Flow Rate
Noise Level
Remote Terminal Unit
Oil levels and Maintenance alarms
Radioactivity levels
Water levels
Temperature

AR-DDoS over IoT

AR-DDoS

Amplified Reflection DDoS

Evolução de DDoS



Fonte: Google Cloud Blog[1]

Amp Reflex DDoS:
Is it feasible/practical abusing IoT mirrors?

- How?
- Plan:
  - Reference implementation
  - Characterize mirror/reflector behavior
    - Saturation: amplification not sustained
  - At first general purpose computers
    - Then move to IoT devices

Mastering the attack cycle...

Striker v1 – MacOS SNMP
Striker v2 – Linux SNMP & SSDP

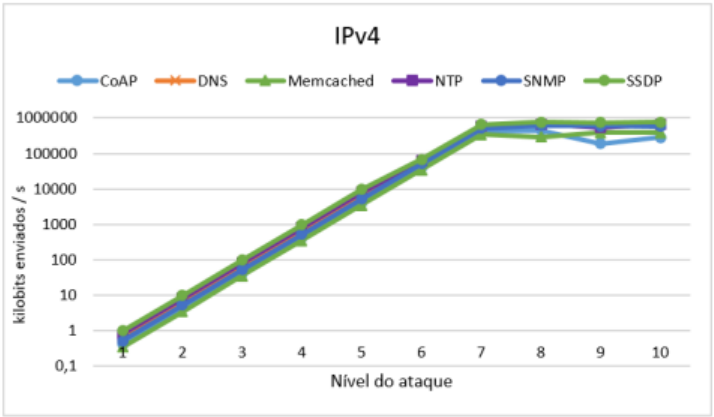
Linderhof

Version 1.0

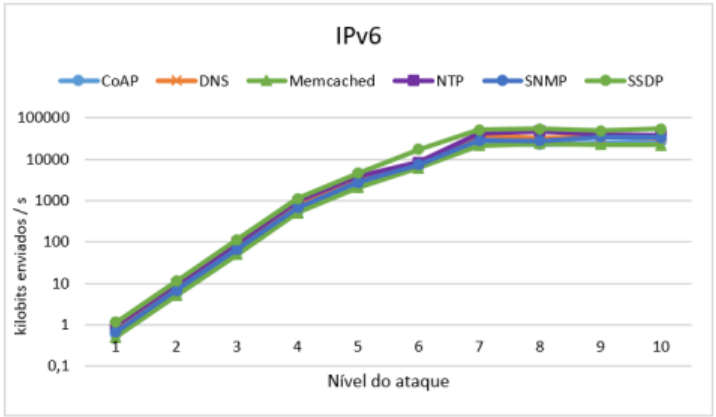
controlled attack
probe Generation
over IPv4 and IPv6

Version 2.0 (Versailles ?)

Carpet bombing
Pulse wave with
shapping
GUI



Kbps gerados - IPv4



Kbps gerados - IPv6

Amplified Reflection DDoS: padrão de saturação de refletor

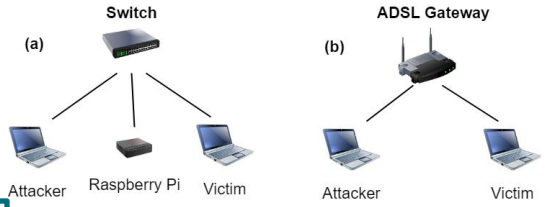
Table 9 Comparison of amplification rates by protocol: values for SNMP, SSDP, NTP, and DNS are from [13]

Protocol	Amp. bits	Amp. pkt	Sat.	Cons.	Amp. res.	Aten.
SNMP	609.03	33.40	3	4	bps and pkt	
SSDP	38.23	10.00	3	4	bit	pkt
NTP (600 hosts)	422.81	100.00	2	3		bps and pkt
DNS (Amp-45)	43.81	3.00	3	4	bps and pkt	
CLDAP	31.36	2.00	3	4	bps and pkt	
Memcache	13629.51	468.00	3	4	bps	pkt

[13] Gondim, J.J.C., Oliveira Albuquerque, R., Sandoval, O.A.L.: Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols. https//doi.org/10.1016/j.future.2020.01.024. Future Generation Computer Systems (2020)

SNMP and SSDP over IoT

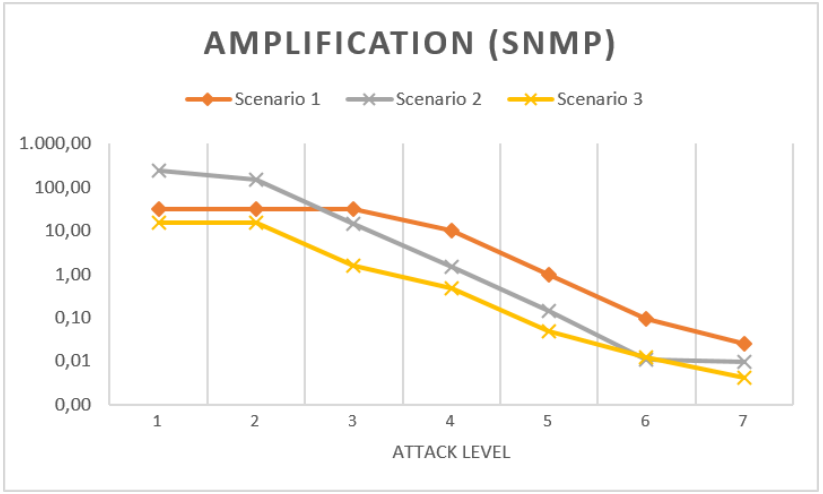
Vasques, Alan Tamer, and João J C Gondim. "Amplified Reflection DDoS Attacks over IoT Mirrors: A Saturation Analysis." 2019 Workshop on Communication Networks and Power Systems (WCNPS). IEEE, 2019

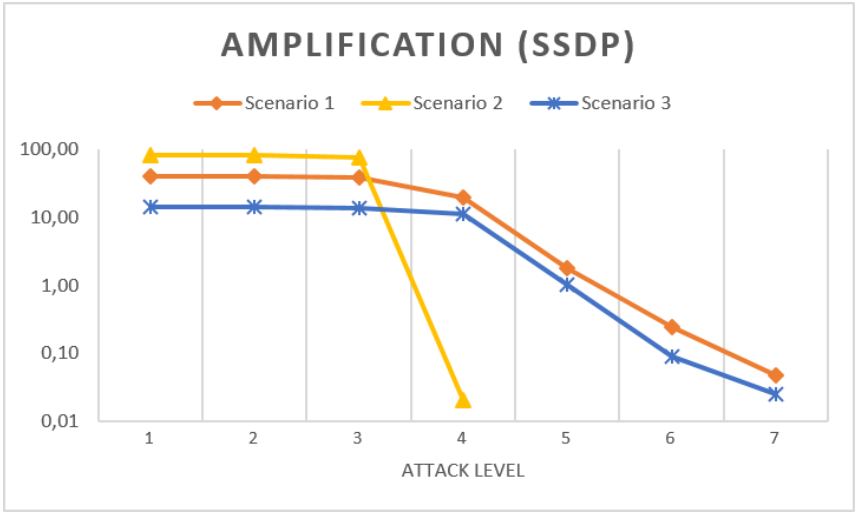


SCENARIO 2 (SSDP)

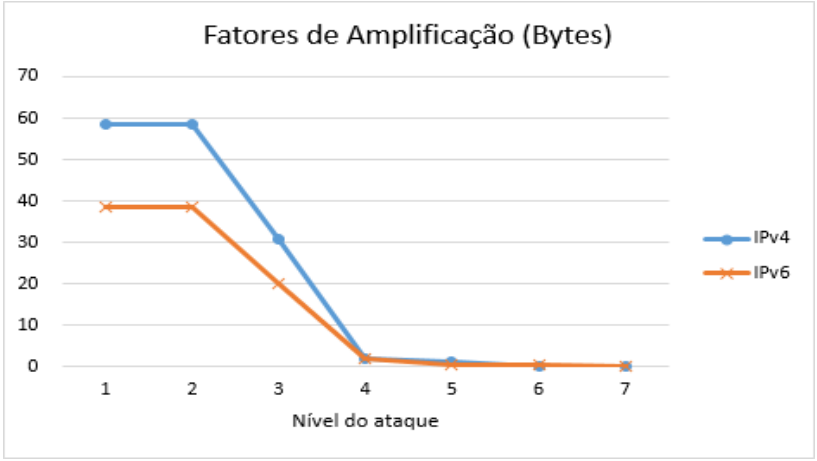
Level	Attacker Outbound			Victim Inbound			Amplification
	Bytes	*Kbps*	*pkt/s*	*Bytes*	*Kbps*	*pkt/s*	
1	1768	1.3	1.2	144560	29.0	9.1	81.76
2	15912	12.0	11.0	1301040	28.9	9.1	81.76
3	161840	119.9	110.2	12432160	28.8	9.1	76.82
4	1604800	1199.7	1102.7	33360	28.0	8.8	0.02
5	15912000	11995.5	11025.3	0	0.0	0.0	0.00
6	106080000	76946.2	70722.6	0	0.0	0.0	0.00
7	122400000	77912.2	71610.4	0	0.0	0.0	0.00

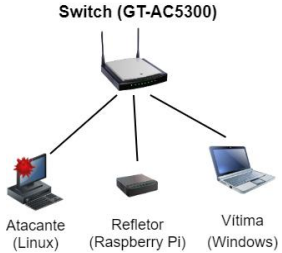
Attack duration
level 1 – 39.9s
level 2 – 360.4s
level 3 – 3447.9s
level 4 – 9.5s

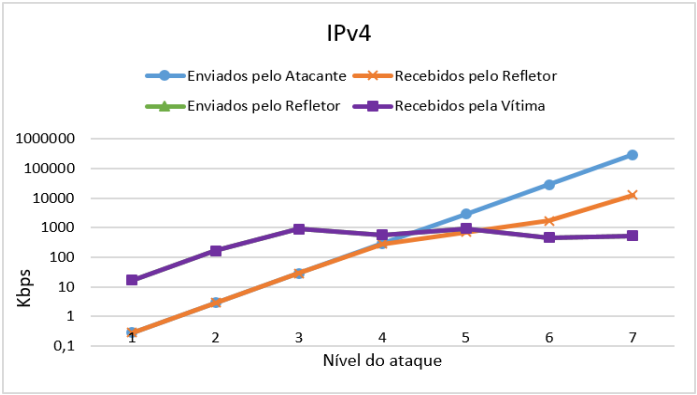


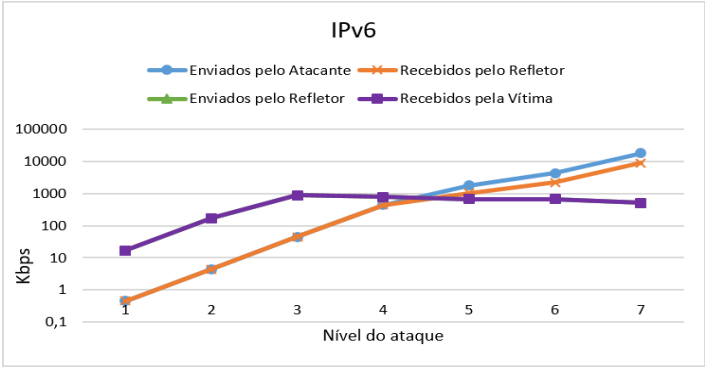


CoAP over IoT





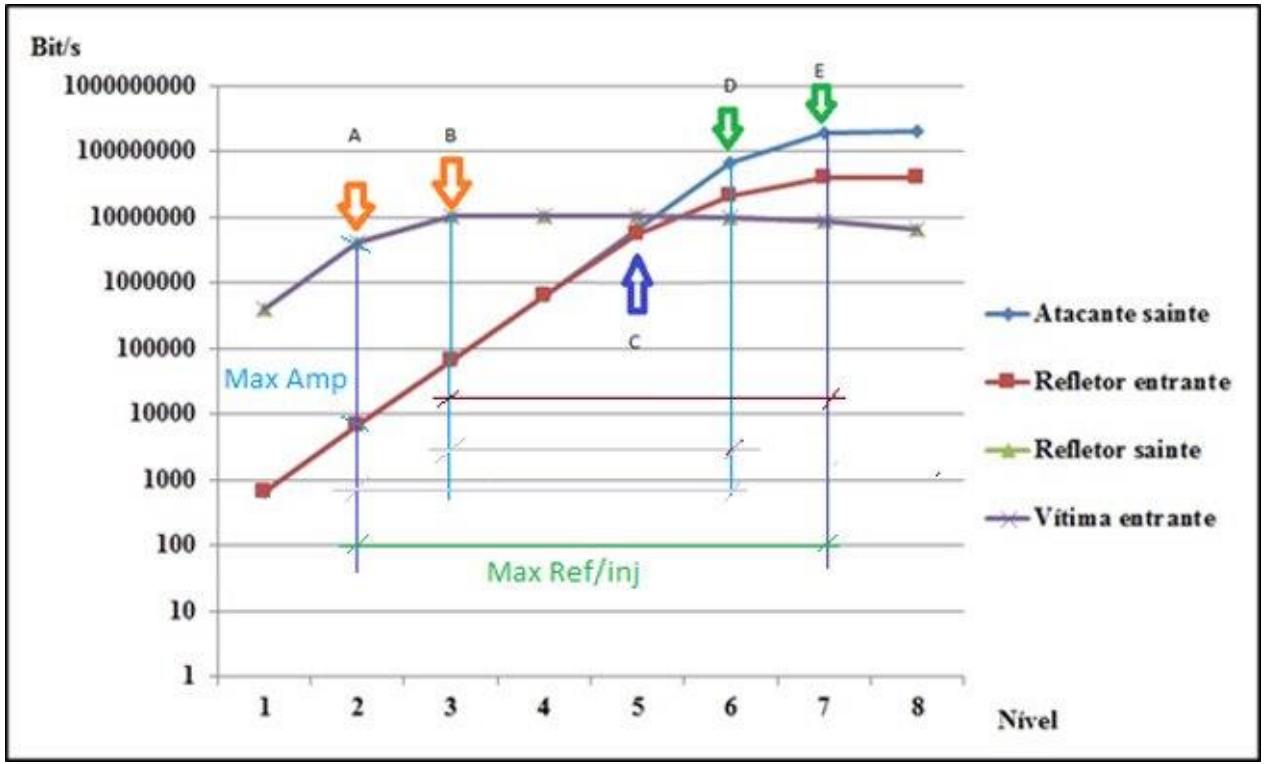




Vasques, A. T. and Gondim, J. J. C. (2020). Ataques ddos por reflexão amplificada sobrerefletor iot rodando coap. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). Submetido e Aceito.

Como coordenar e operar um AR-DDoS com uma botnet de +100 mil bots IoT?

AR-DDoS Reflector behavior Dynamics



Mitigation and Detection

Mitigation

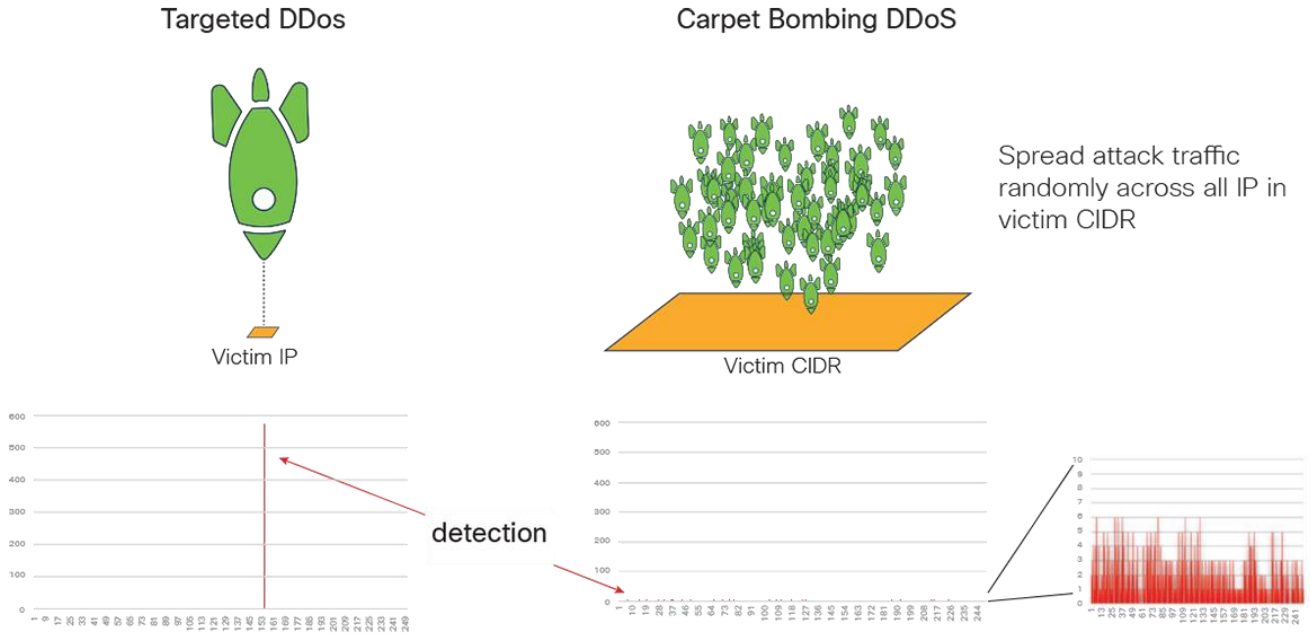
Two main techniques

Black Holing

Hybrid Cloud/CDN

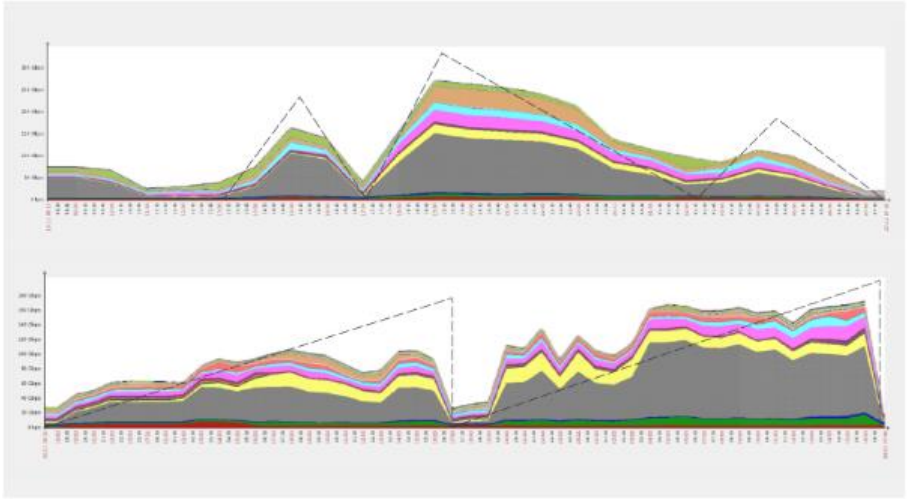
Carpet Bombing

Stress on Blackholing



https://www.cisco.com/c/dam/en/us/products/collateral/security/evolution-ddos-attack-vectors-wp.docx/_jcr_content/renditions/evolution-ddos-attack-vectors-wp_12.png

Pulse Wave DDoS Attack



Stress on hybrid mitigation

Implications for **Detection**, Mitigation, and Security Management

- based on rate: thresholds would have to operate at lower values

-> poorer detection: attack flows become less distinguishable from normal flows

- based on machine learning: data sets used in training will have to be updated to include flows with this characteristic

-> model retraining will be necessary.

- using heuristics: based on other flow characteristics (large numbers, hundreds to thousands, of unsolicited replies from severaldifferent origins)

-> should be less affected.

Implications for Detection, **Mitigation**, and Security Management

- For DDoS in general, but also applicable for AR-DDoS

1 - Origin Side Ingress Filtering: only partially adopted since the benefits are not for the origin network but rather other networks
2 - Destination Side Ingress Filtering: normally affects legitimate users similarly to the DDoS attack it intends to mitigate
3 - Response Rate Limiting: might also impact users but less severely

- 1 not affected
- 2 and 3 will require improved detection with precise source identification is crucial to their deployment without undesirable side effects.

Implications for Detection, **Mitigation**, and Security Management

- Flow filtering and blocking,
  - carpet-bombing and pulse wave tactics already take advantage of them to potentialize attack impact.

  -> DDoS has become security-aware and sophisticated
  - as currently used focus on the effects of DDoS attacks but not the causes:

  filtering on or close to the target/victim does not deal with link saturation

  -> detection, and blocking far from the target and closer to the origin.

  -> but that might be impractical.

- A compromise between improved efficiency and reduced undesirable side effects:

  -> block flows on converging points along the path to the target.

Implications for Detection, Mitigation, and **Security Management**

- SDNs offer the tools for the aboveimprovements
- intense research on DDoS detection and mitigation
- so far, proposed solutions fall short of improving existing solutions incurring in similar issues:
  - ineffective or wrong detection
  - unfeasibility for real-time deployment
  - blocking that does not address link saturation placed either close to the victim or affecting other nodes in the network.

How about SDN combined with Fog/Edge Computing?

Mostly for IoT environment

Fog/Edge Computing:

- GW + DMZ
- IoT on a seggregated network

SDN

Blocking egress traffic: spooffed traffic

A “revamp” of BCP38

Implications for Detection, Mitigation, and **Security Management**

Summarizing:

detection and mitigation must shift to identifying attack sources and convergence points
to improve precision and overall efficiency in defending against volumetric DDoS.

O futuro é brilhante (I)

We </3 Cloud: Denial of Wallet Attacks

The attack would not take the site down, but will make the teams have a not so fun month.

It's not only AWS; this work on Azure, GCP, Alibaba Cloud, and Oracle Cloud.

O futuro é brilhante (II)

We </3 Cloud: Adventures in Bahrain?

You can run a single AWS API call to launch SQL server in Bahrain (me-south-1), and it would cost an upfront payment of $3,118,367 USD.

Conclusion

Attacker perspective:

- can control the reflectors and modulate the attack at his will
- the complexity of performing such attacks requires no deep knowledge of the abused protocols or defenses that could be in place.

Mitigation strategies may vary from the complexity of the infrastructure to the availability of human resources with the knowledge to interfere in the network without compromising available resources or amplifying the damage.

Conclusion

For an attacker to generate a volume of traffic with less attack effort, he would need a greater number of reflectors.

Demands enhanced command and control capabilities.

Use reflectors hosted in the cloud (?)
Shifts the focus of prevention, detection, and mitigation to the scope of cloud security.

IoT devices as reflectors, or possible injectors, covering a larger base of devices, which, in turn, brings more capacity to the attackers and more complexity to the defenders

Coming attractions:

- TCP focused DDoS:
  Middleboxes: reflection
  HTTP/2 atacks
- Denial of Wallet attacks:
  Cloud + APIs + microservices +
  poor [apps (queries) + poor DB design]
- Generative Adversarial AI-driven Malware
  (cats and churches)
  Whitehat botnets
  Resilient Command-and-Control

Clique para adicionar um título