Global 5G event

Cyber Attack in IoT on the rise

- Security in 5G applications –

Koji Nakao

Distinguished Researcher - NICT

Guest Professor - Yokohama National University

2017/5/24

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

The Internet of Things (IoT
upon us. Everything from
home appliances, watches
even children's toys are be
connected online. It is proj
that by the year 2020, ther
be more 25 billion devices

IoT Home Routers Botnet Leveraged in Large **DDoS Attack**

SucuriSecurity | sucuri.ne

Home Router Botnet Leveraged in
Large DDoS Attack

Is your refrigerator really part of a massive spam-sending botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices

by Dan Goodin - Jan 18, 2014 5:25am JST

Internet of Things security conce
boost in IoT services

by

News roundup: As Internet of Things conce
rise reality, one vendor is quick to
to combat the risks. Plus: 1% of use
e risk; Target pays up; Apple devic
ly secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Internet of Things" is the new Windows XP —malware's favorite target

Devices attacked our honeypot during Jan-June 2016

Categories of Inferred Infected devices (2016.9)

- Surveillance camera
  - IP camera
  - DVR
- Network devices
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances
- Telephone
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters
- Infrastructures
  - Parking management system
  - LED display controller











Devices are inferred by telnet/web banners

- Control system
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)

Home/indivisuals

- Web cam, Video recorders
- Home automation GW
- Solar Energy Control System
- Energy demand monitoring system


- Broadcasting
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box,



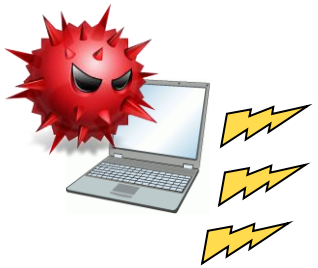
- Etc
  - Heat pump
  - Fire alert system
  - Medical device (MRI)
  - Fingerprint scanner

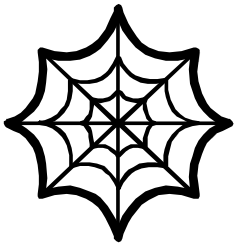
ROUTE CAUSES OF THE MASS-INFECTION

Telnet

Darknet monitoring

Darknet: unused but routable IP address (es) or net blocks





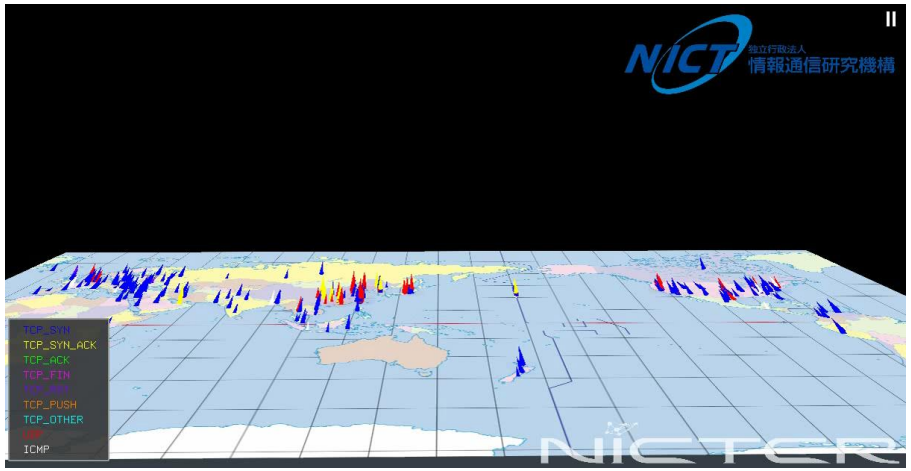
Many researchers/organization utilize darknet to monitor malicious activities like scanning, remote exploits, back scatters, etc

Scanning observation by nicter-Atlas

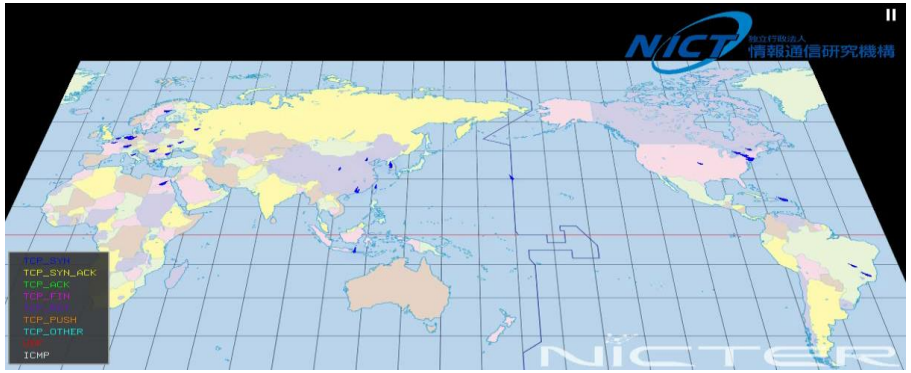
Recently, “scanning to Port 23 (telenet)” is getting larger!!

- Capturing packets through dark-net in real time basis.
- Color indicates the protocol types.

UDP
TCP SYN
TCP SYN/ACK
TCP Other
ICMP



Atlas All view



Atlas only port23

Increases of telnet attacks

packets

7
6
5
4
3
2
1

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	2,699,639	45%
22	461,738	8%
80	348,077	6%
1433	208,460	3%
3306	199,372	3%
3389	151,868	3%
8080	145,657	2%
443	124,800	2%
9200	116,255	2%
25	94,901	2%

1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

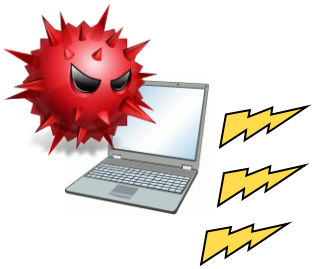
TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	11,727,894	65%
1433	791,485	4%
22	559,059	3%
3389	247,547	1%
80	247,159	1%
8080	184,132	1%
443	147,434	1%
3306	128,382	1%
4028	116,029	1%
54628	78,378	0%

10 years observation of NICTER darknet (23/tcp only)

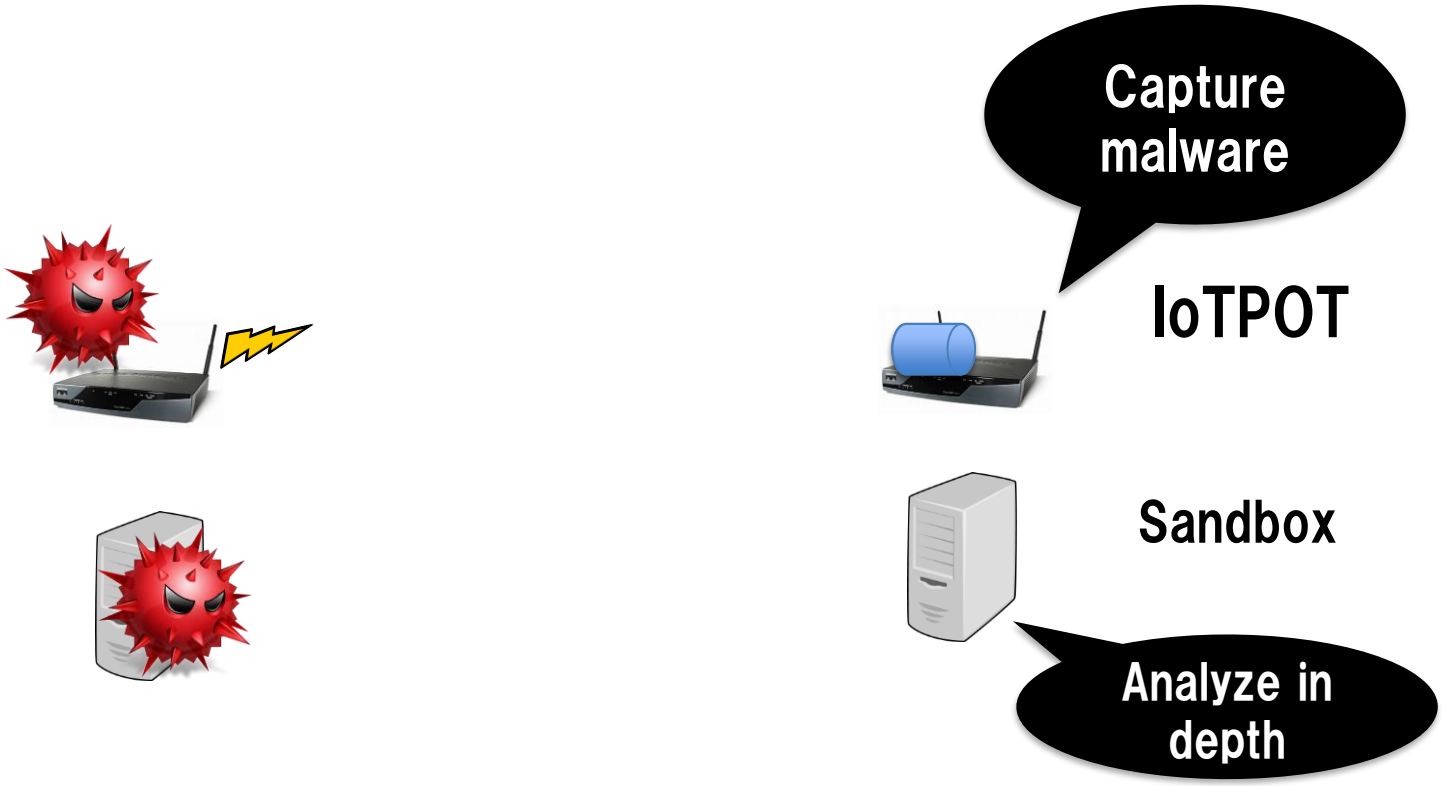
To monitor in depth

Darknet monitoring is simple and great to monitor wider networks but limited as it only gets the first packet of each attack.



Our system: IoTPOT = IoT Honeypot

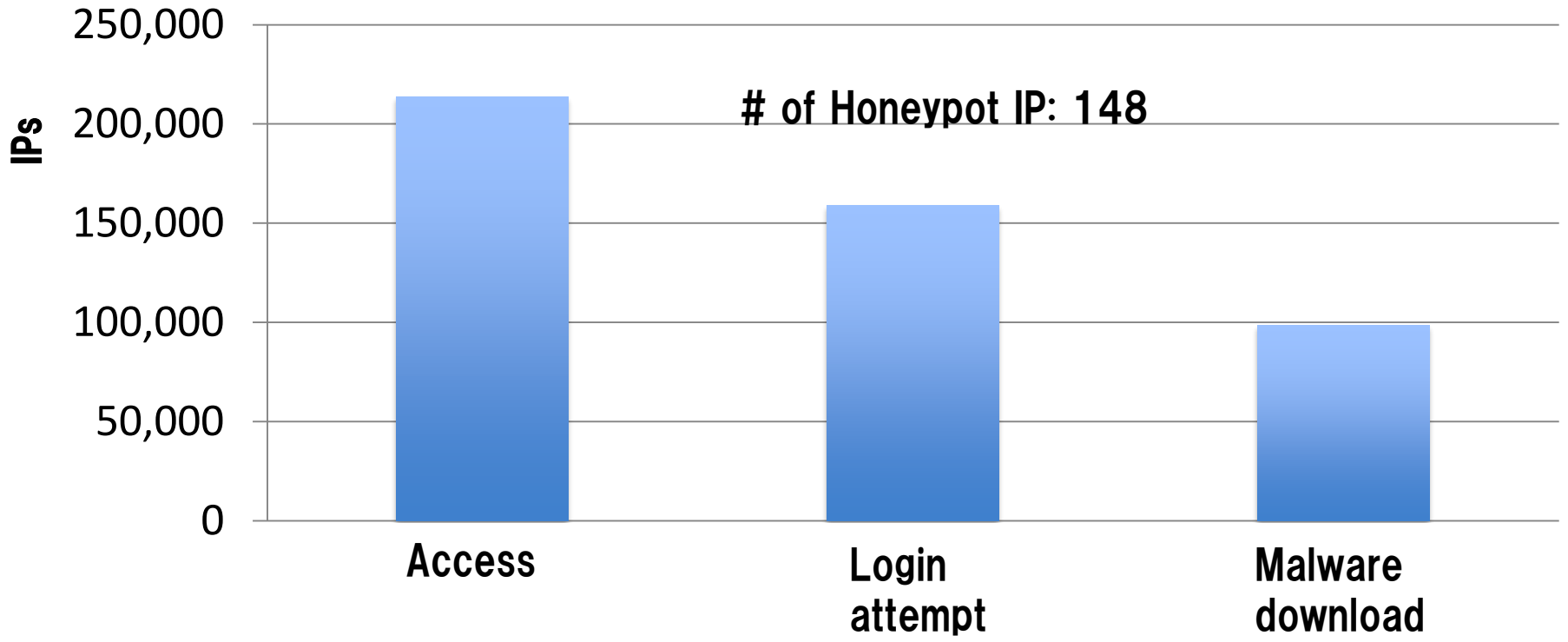
We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

Observation result (last year)

Period:2015/4/1～2015/7/31 (122days)

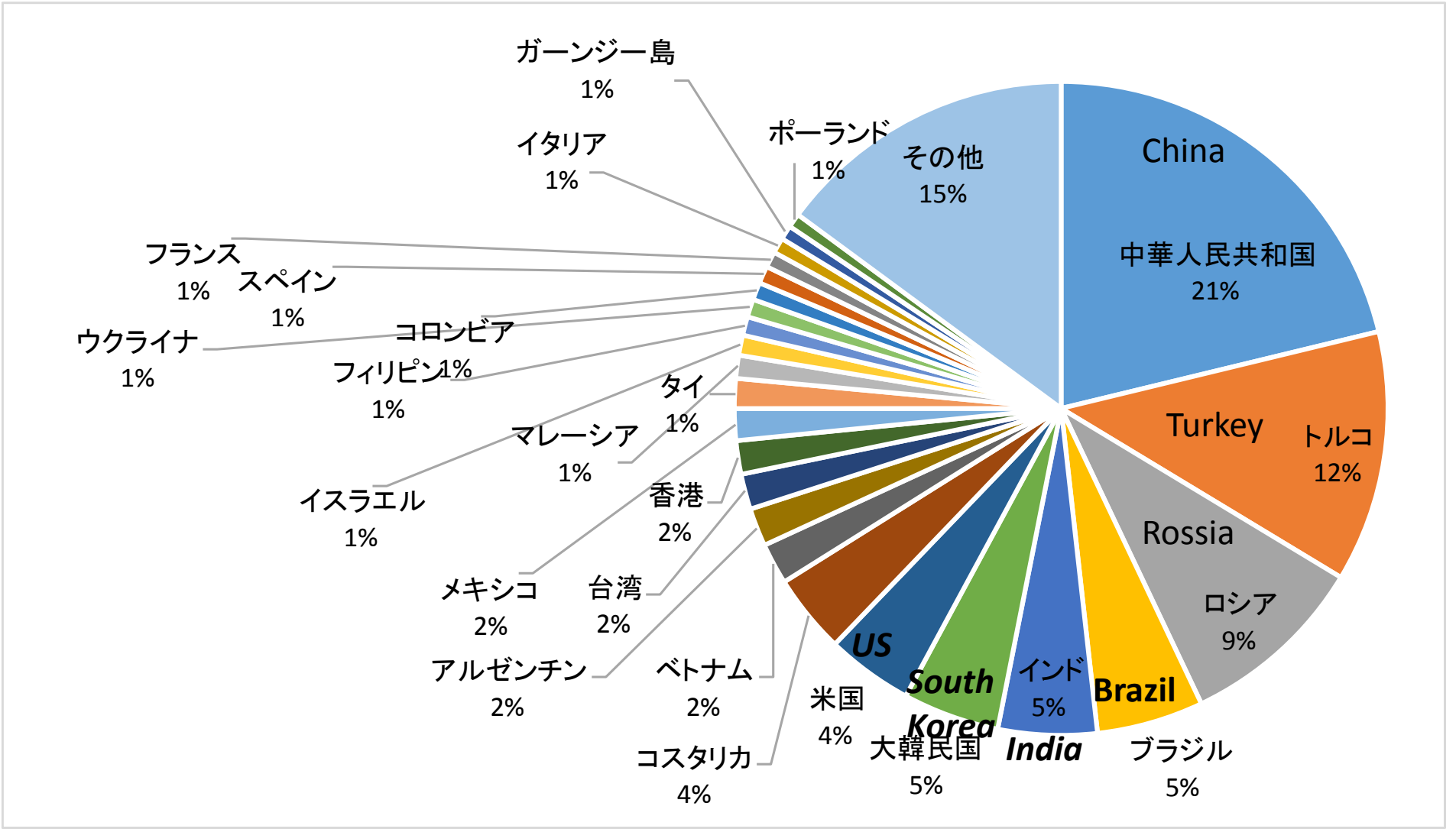


150,000 IPs attempted to login, 100,000 actually did send us malware binaries

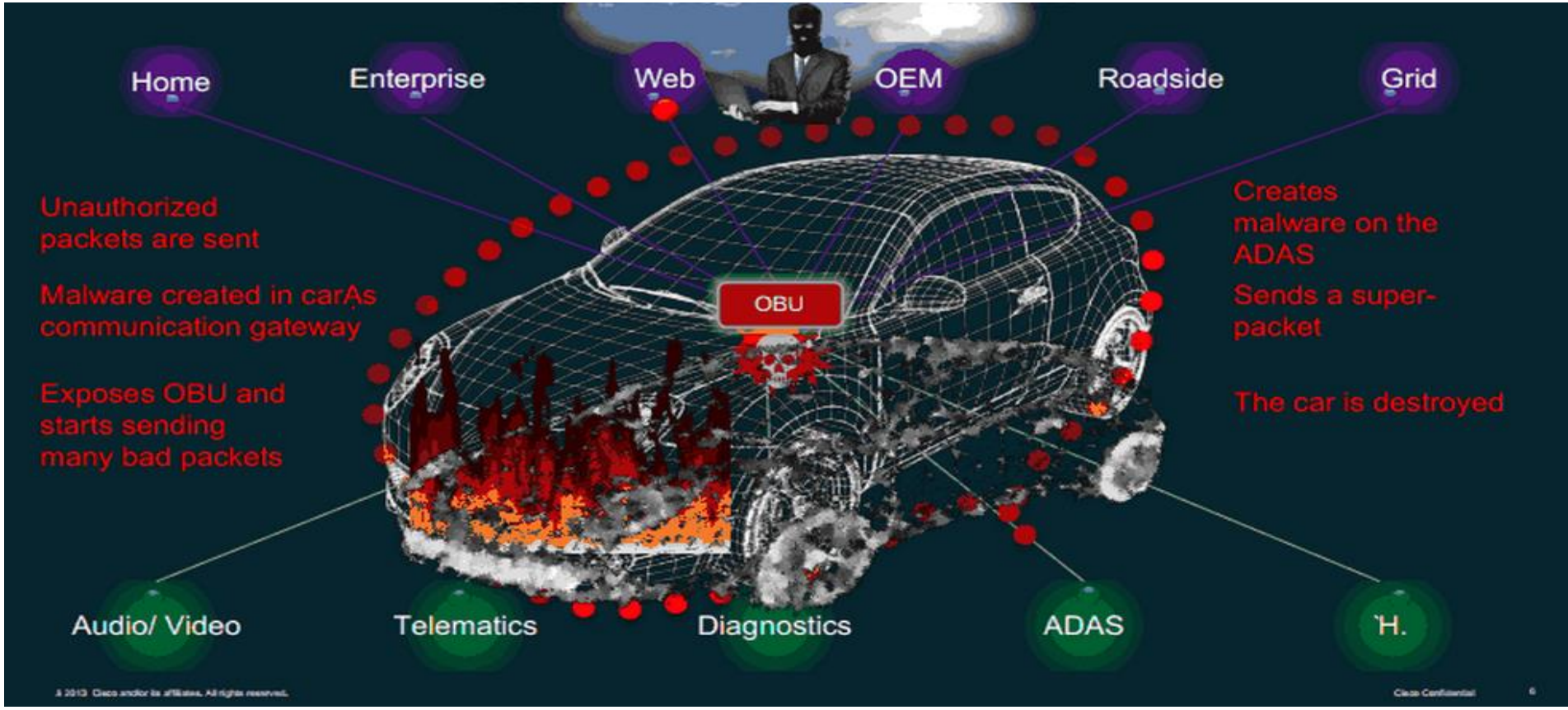
Binaries with 11 different CPU architectures
93% of the binaries were new in VT (as of 2015/9/24)

Source countries

Period:2015/05/01 - 2016/02/21



Introduction of Connected Vehicle Communications as an Use-Case of 5G



Threats against networked vehicle

Each New Connection or Device Adds a Potential Target!!

Much data to be protected!

V2X Communication Data

http://telematicswire.net/connected-cars-and-smart-homes-coherence-of-a-convergence-platform/

National Institute of Information and Communications Technology

Attack from the remote in the case of FIAT Chrysler's Jeep Cherokee

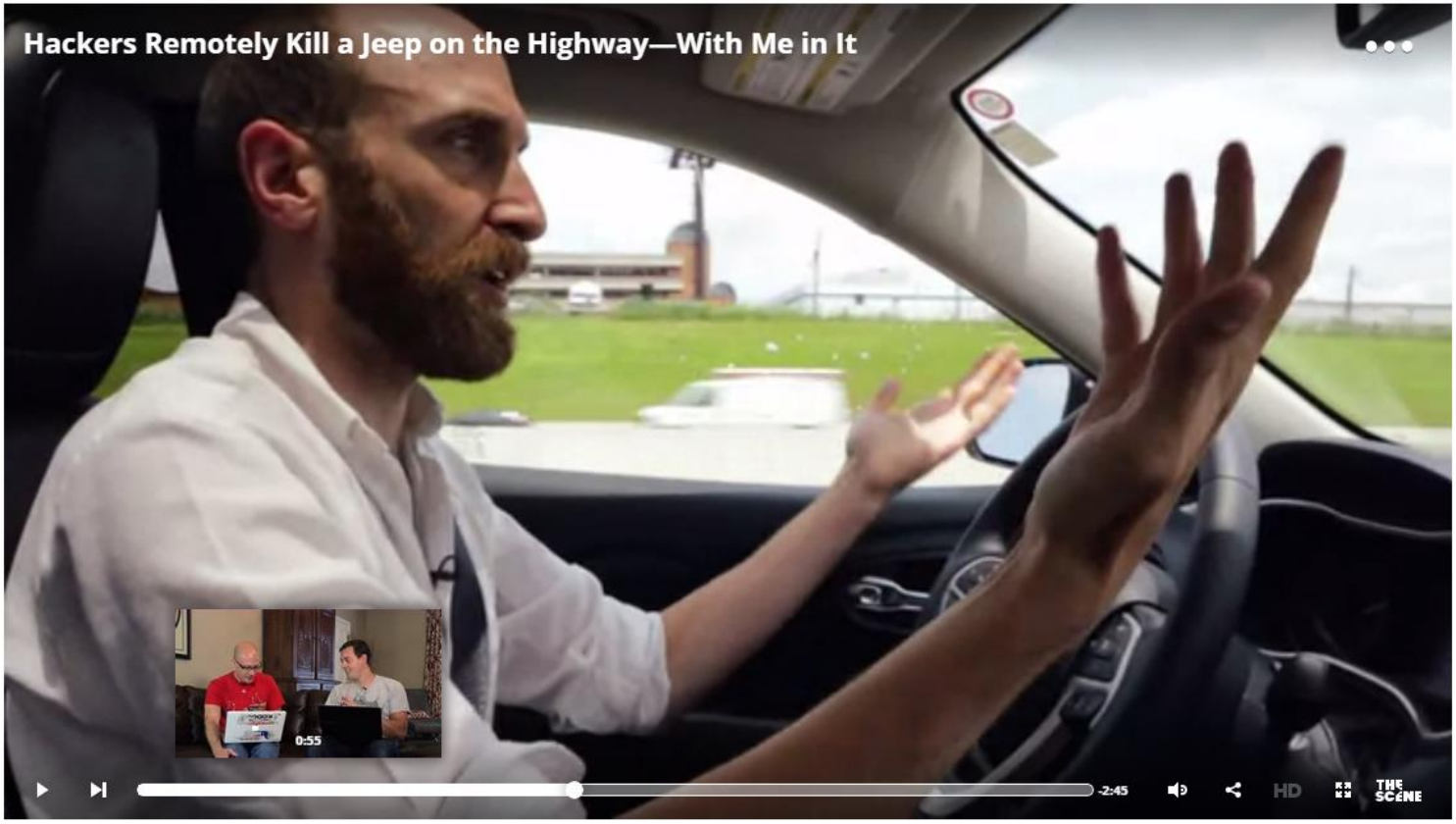
WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Remote exploitation against Jeep Cherokee (cont.)

- **Research activity by two hackers**
  - Presented at Black Hat USA 2015 (5–6, Aug)
    - "Remote Exploitation of an Unaltered Passenger Vehicle"
    - Charlie Miller, Security Engineer, Twitter
    - Chris Valasek, Director of Security Intelligent at IOACTIVE, INC.

- **Demonstration of attacks against FIAT Chrysler's Jeep Cherokee**
  - **Remote exploit attack against an Internet-connected device (UConnect) → A kind of IoT device**
  - Remotely controlled the vehicle on the highway
    - Abuse a steering wheel
    - Abuse brake and accelerator
    - On/Off of the engine

What security controls should be considered!

- In the context of connected vehicle communications, there are many security controls which should be considered for future car environment as follows:
  - Cryptography implementation
  - Authentication deployment
  - Key management
  - Firewall/IPS controls
  - Vulnerabilities management
  - Security risk management, threats management and vulnerabilities management
  - **Secure software updates**
  - Etc.…
  - **In the case of "automatic driving (vehicle)", there will be strong connection *with the use of 5G NW*.**

National Institute of Information and Communications Technology

Many Application/services using IoT: For Smart+Connected City Infrastructure

Smart+Connected City Parking

Give citizens live parking availability information to reduce circling and congestion

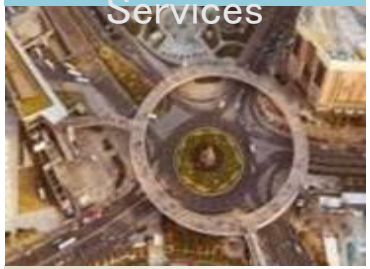
Smart+Connected City Traffic

Monitor and manage traffic incidents to reduce congestion and improve livability

Smart+Connected City Safety & Security

Automatically detect security incidents, shorten response time, and analyze data to reduce crime

Smart+Connected City Location Services



Provide view of people flow data to aid planning and leverage location data for contextual content and advertising

Smart+Connected City Lighting

Manage street lighting to reduce energy and maintenance costs

Utilization of IoT will have strong connections with the Use Cases by means of 5G environment (like automatic driving)

Secure Design Approach for 5G

Basic:

1. Identification of use cases for 5G application;
2. Threat Analysis (Assessment) of each Use Case;
3. Recognition of a set of Security Requirements for the Use Case;
4. Study and develop security controls (countermeasures) based on the security requirements.

Dependent of Security Requirement, *Lightweight Crypto* might be one of the important security controls for 5G NW.

Specific:

a. Design 5G services with security consideration (security by design) based on the above basic approach;
b. Monitor and observe the 5G services;
c. Improve the security controls and continuous monitoring

National Institute of Information and Communications Technology

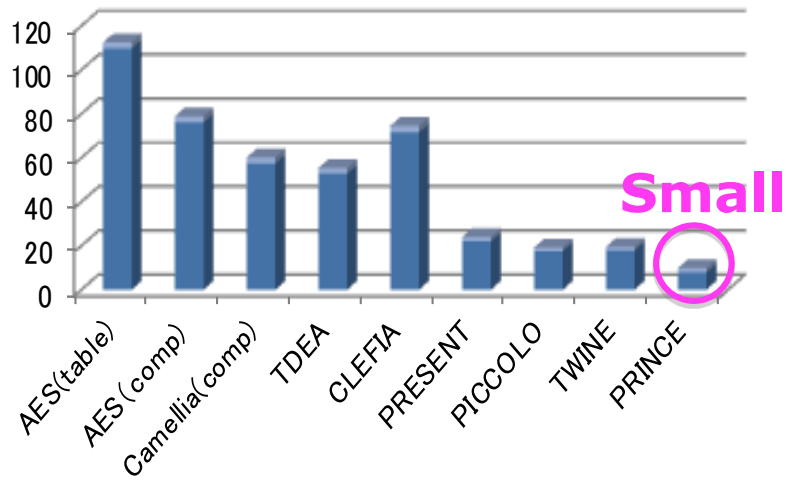
Why Lightweight Cryptography is considered…

	AES	Lightweight block ciphers
Properties		
Block Size	128 bits	64 bits
Key Size	128/192/256 bits	80-128 bits
Key Schedule		Light (Simple)
S-box	8 x 8	4 x 4
Hardware Implementation		
Gate Size (ASIC)	3-10 Kgate	< 3 Kgate
latency		< 20ns within 10Kgates
Software Implementation (on microcontrollers)		
ROM (Enc+Dec)	1KB	< 200B

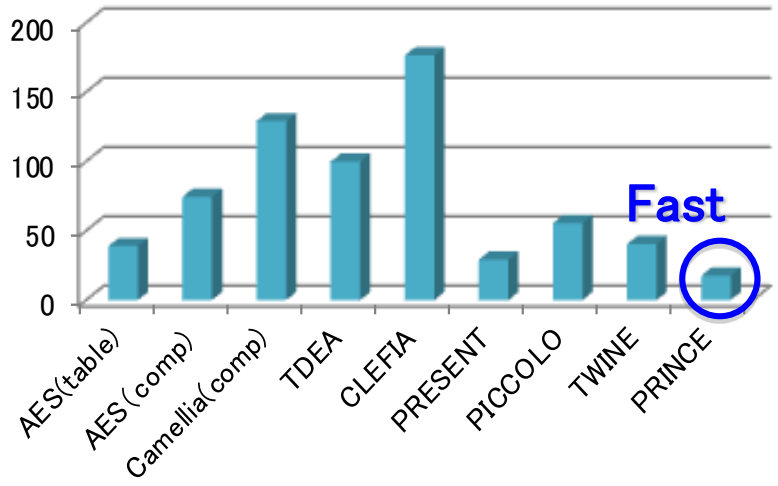
Lightweight Cryptography in the case of ITS…

- Real-time response is crucial in Advanced Driver Assistance Systems (ADAS).
- AES can't achieve encryption in dozens of nano-seconds within dozens of kgates.

Chip Area [Kgate]



Latency [ns]



National Institute of Information and Communications Technology

Secure Design Approach for 5G

Basic (general):

1. Identification of use cases for 5G application;
2. Threat Analysis (Assessment) of each Use Case;
3. Recognition of a set of Security Requirements for the Use Case;
4. Study and develop security controls (countermeasures) based on the security requirements.

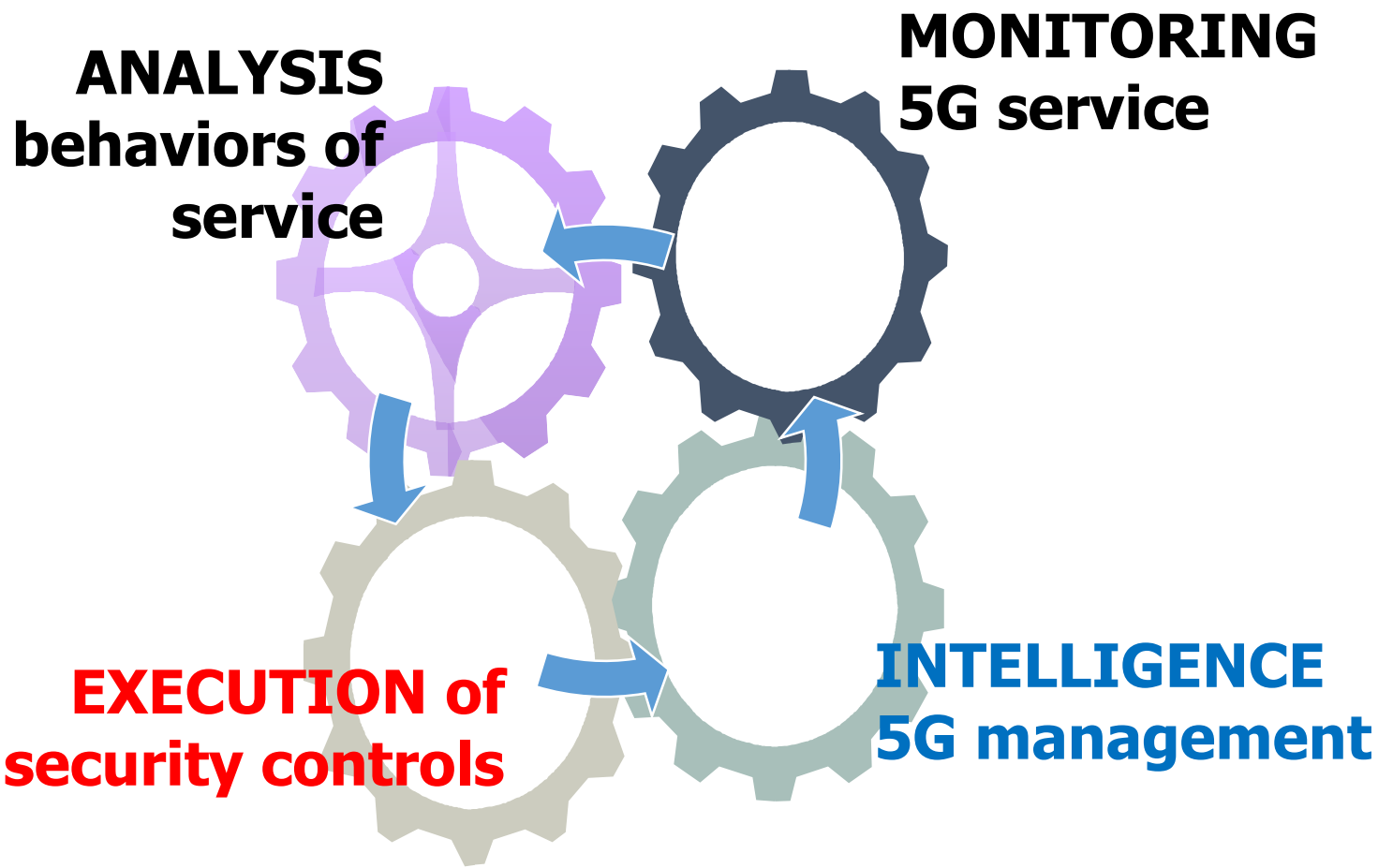
Dependent of Security Requirement, *Lightweight Crypto* might be one of the important security controls for 5G NW.

Specific:

a. Design 5G services with security consideration (security by design) based on the above basic (general) approach;
b. Monitor and observe the 5G services;
c. Improve the security controls and continuous monitoring

National Institute of Information and Communications Technology

Management Process for the 5G service/application



Security Standardization: Scope of ITU-T SG17

- **Security**
  - cybersecurity
  - security management
  - countering spam
  - protection of personally identifiable information
  - security of applications and services for the IoT, smart grid, smartphone, software-defined networking (SDN), Internet Protocol television (IPTV), web services, **ITS**, cloud computing, big data analytics, mobile financial system and telebiometrics
- **Identity management (IdM)**
- **Languages and description techniques**

ITU-T Study Group 17
Security

ITU-T SG17 Management Team (as appointed by WTSA-16)

For the new study period (2017 – 2020)

Chairman	Heung Youl YOUM	Korea (Republic of)
Vice-Chairmen (9)	Mr. Y. Miyake	Japan
	Ms. I. Furey	The United States
	Mr. V. Dolmatov	Russian Federation
	Mr. G. LIN	P.R. China
	Mr. P-K. Kettin-Zanga	Central African Republic
	Ms. W. Latrous	Tunisia (Republic of)
	Mr. Mohamed M.K. ELHAJ	Sudan
	Mr. G.Evren	Turkey
	Mr. H.D.Miguel	Argentina

Questions in ITU-T SG 17

- WTSA-16 confirmed the 13 Questions of SG17:

Question number	Question title	Status
1/17	Telecommunication/ICT security coordination	Continuation of Q1/17
2/17	Security architecture and framework	Continuation of Q2/17
3/17	Telecommunication information security management	Continuation of Q3/17
4/17	Cybersecurity	Continuation of Q4/17
5/17	Countering spam by technical means	Continuation of Q5/17
6/17	Security aspects of telecommunication services and networks	Continuation of Q6/17
7/17	Secure application services	Continuation of Q7/17
8/17	Cloud computing security	Continuation of Q8/17
9/17	Telebiometrics	Continuation of Q9/17
10/17	Identity management architecture and mechanisms	Continuation of Q10/17
11/17	Generic technologies (Directory, Public-Key Infrastructure (PKI), Privilege Management Infrastructure (PMI), Abstract Syntax Notation 1 (ASN.1), Object Identifiers (OIDs)) to support secure applications	Continuation of Q11/17
12/17	Formal languages for telecommunication software and testing	Continuation of Q12/17
13/17	Security aspects for Intelligent Transport System (ITS)	New Question

ITU-T Study Group 17
Security

WP Structure of SG17

- **Q1/17Telecommunication/ICT security coordination**

- **Working Party 1 "Telecommunication/ICT Security"**
  - **Q2/17 Security architecture and framework**
  - Q3/17 Telecommunication information security management
  - Q6/17 Security aspects of telecommunication services and networks
  - **Q13/17 Security aspects for Intelligent Transport System**

- **Working Party 2 "Cyberspace security"**
  - Q4/17 Cybersecurity
  - Q5/17 Countering spam by technical means

- **Working Party 3 "Application security"**
  - Q7/17 Secure application services
  - Q8/17 Cloud computing security
  - Q12/17 Formal languages for telecommunication software and testing

- **Working Party 4 "Identity management and authentication"**
  - Q9/17 Telebiometrics
  - Q10/17 Identity management architecture and mechanisms
  - Q11/17 Generic technologies to support secure applications

ITU-T Study Group 17
Security

Conclusion for New Services/Applications under 5G

Follow the proposed security approach:

1. **Identification of Use Cases**
2. **Threat analysis**
3. **Security Requirements**
4. **Security Controls**

In addition to the above approach:

a. **Threat observation/analysis and Vulnerability detection**
b. **Malware/intrusion detection**
c. **Remote curing method for vulnerable services/systems**
d. **Remote OTA Software Update**
e. **Data Confidentiality**
   – Light-weight crypto
f. **Appropriate Authentication and Access control (including IdM)**
g. **Incident handling and Information (threat) sharing**
h. **etc…**

Thank you for listening