Konsep Sistem Keamanan Komputer

Dr. Andreas Hadiyono, ST, MMSI

Cyber Security

- Cyber crime cost could hit $6 Trillion annually by 2021.
- Over 169 million personal records were exposed in 781 publicized breaches in 1015
- In 2015 38 percent more security incidents detected in 2015 than in 2014
- Majority (91.3%) of malware use DNS to carry out attack
- Browser extensions are used to steal data and account information
- Use of HTTPS is increasing reducing the effectiveness of firewalls

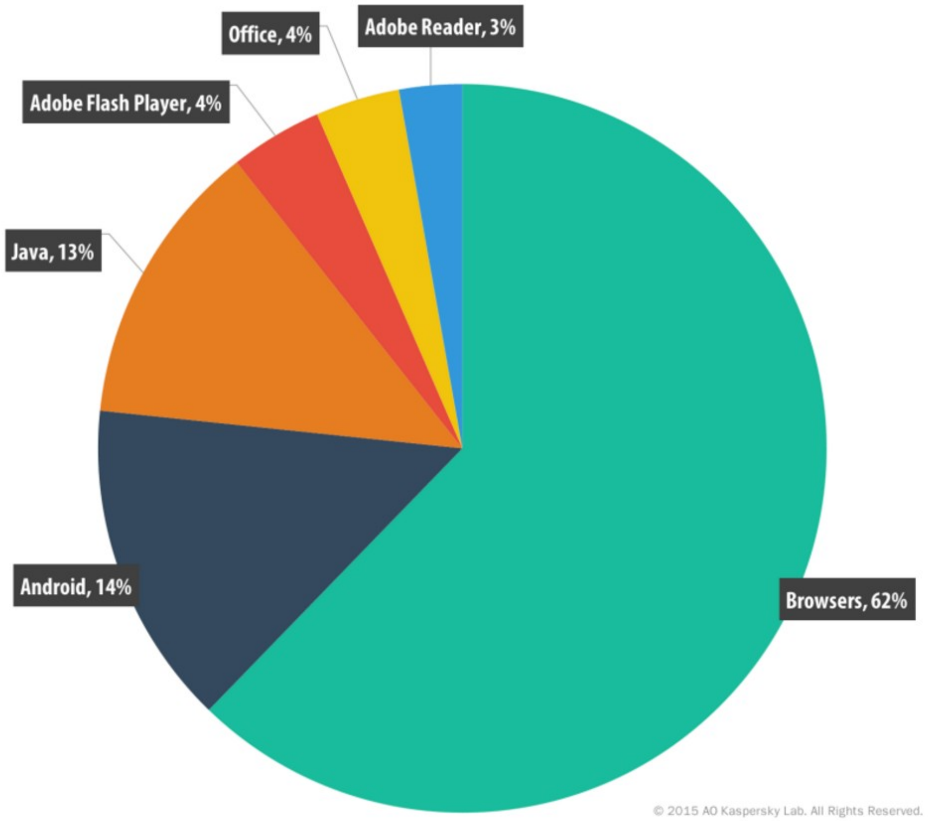
Cyber Warfare

- Security of computers, companies, smart grid, and nations
- Nation States are penetrating other nations computers
- 5th domain of warfare (after land, sea, air, space)
- In 2010, US set up US Cyber Command
- UK, China, Russia, Israel, North Korea have similar centers
- Many cyber wars: North Korea vs. USA, Israel vs. Syria, South
- Korea vs. North Korea, India vs. Pakistan, ...
-

The computer security problem

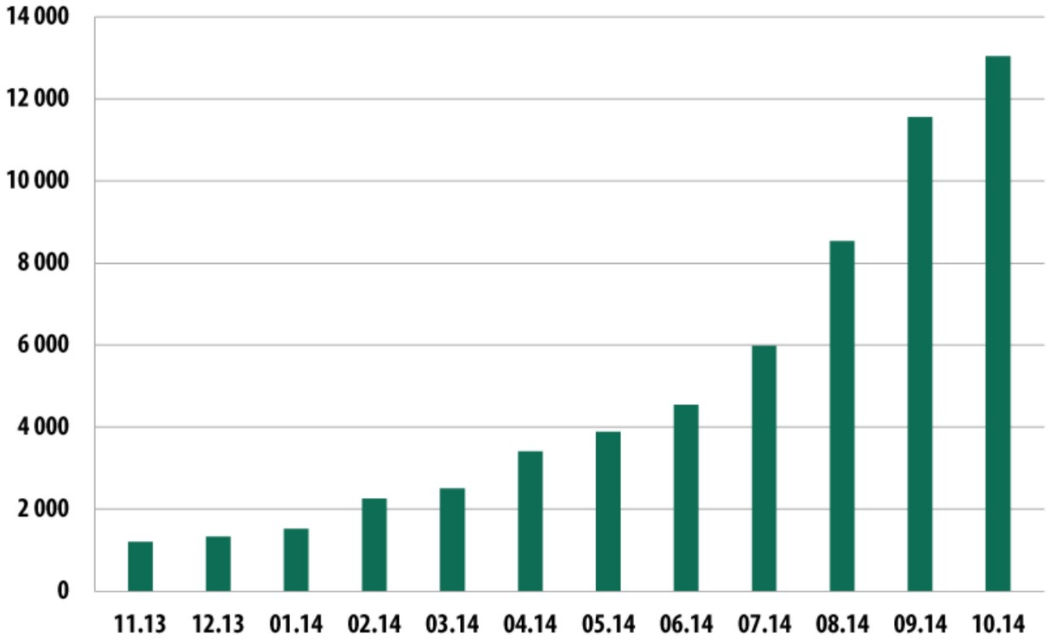
- **Lots of buggy software**
- **Social engineering is very effective**
- **Money can be made from finding and exploiting vulns.**
  - Marketplace for vulnerabilities
  - Marketplace for owned machines (PPI)
  - Many methods to profit from owned machines

Vulnerable applications being exploited



© 2015 AO Kaspersky Lab. All Rights Reserved.

Mobile malware (Nov. 2013 – Oct. 2014)



The rise of mobile banking Trojans (Kaspersky Security Bulletin 2014)

Why own machines:
1. IP address and bandwidth stealing

- Attacker’s goal: look like a random Internet user

- Use the IP address of infected machine or phone for:

- **Spam** (e.g. the storm botnet)
  - Spamalytics: 1:12M pharma spams leads to purchase
  - 1:260K greeting card spams leads to infection

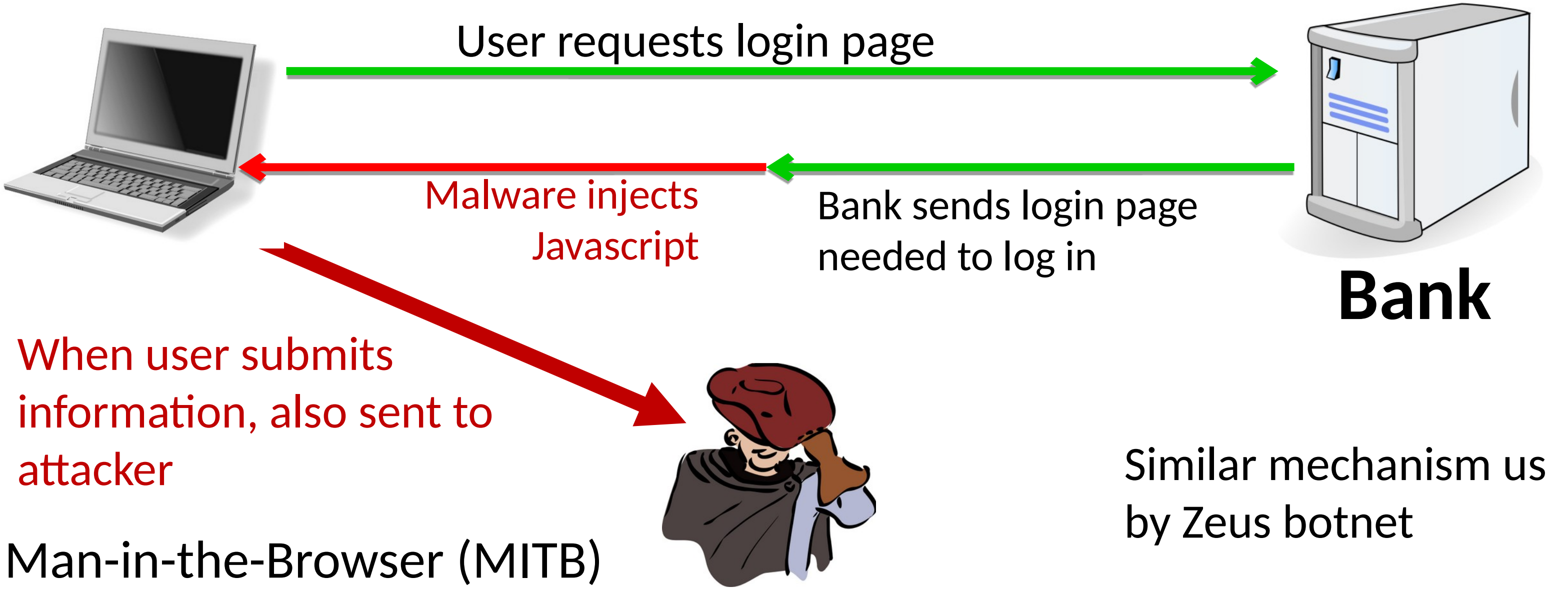
- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)
- **Click fraud** (e.g. Clickbot.a)

Why own machines:

2. Steal user credentials and inject ads

keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (and many like it)



User requests login page

Malware injects Javascript

Bank sends login page needed to log in

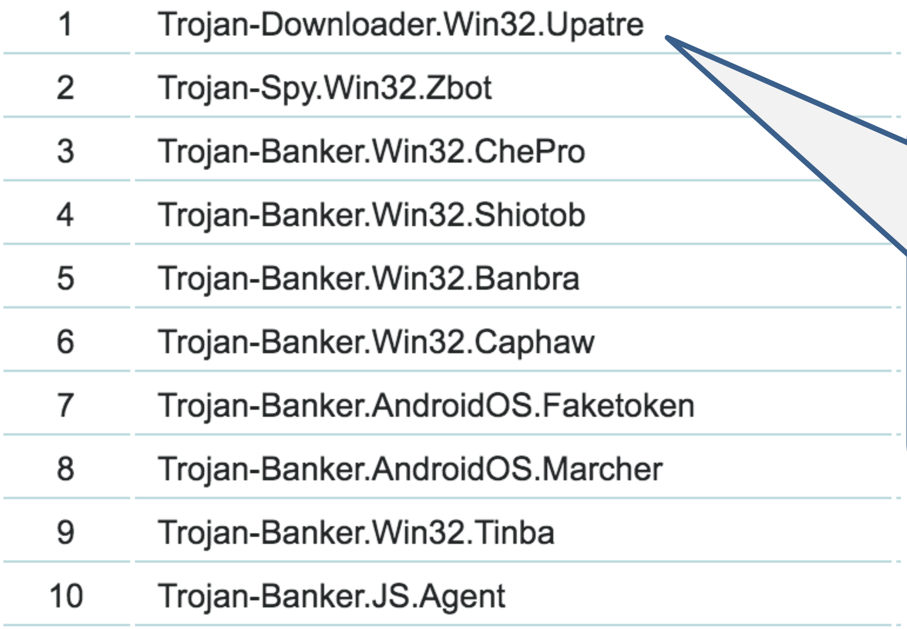
Bank

When user submits information, also sent to attacker

Man-in-the-Browser (MITB)

Similar mechanism used by Zeus botnet

Lots of financial malware

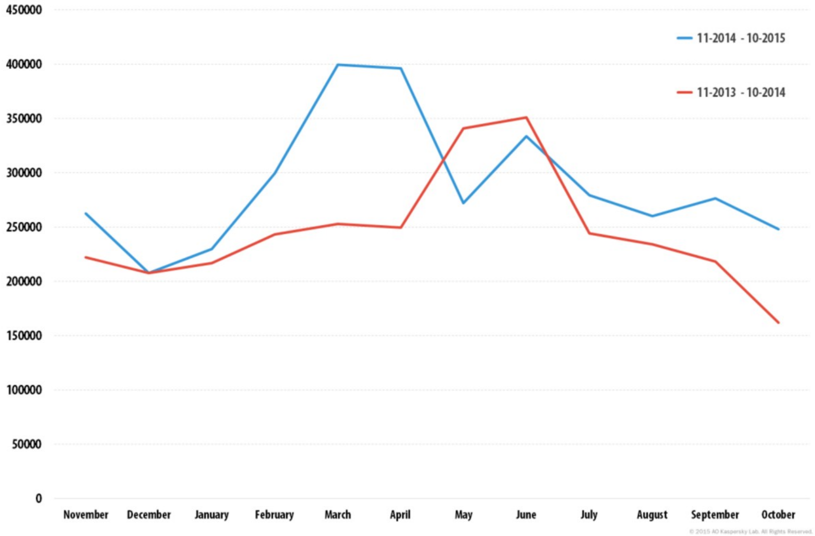


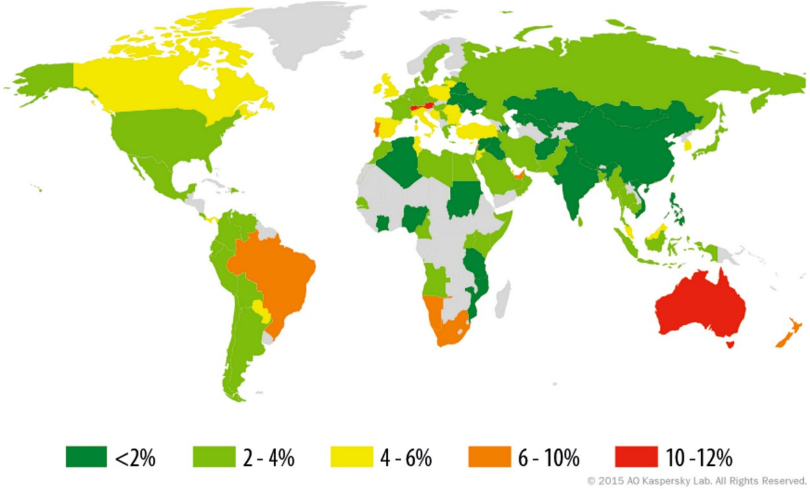
1	Trojan-Downloader.Win32.Upatre
2	Trojan-Spy.Win32.Zbot
3	Trojan-Banker.Win32.ChePro
4	Trojan-Banker.Win32.Shiotob
5	Trojan-Banker.Win32.Banbra
6	Trojan-Banker.Win32.Caphaw
7	Trojan-Banker.AndroidOS.Faketoken
8	Trojan-Banker.AndroidOS.Marcher
9	Trojan-Banker.Win32.Tinba
10	Trojan-Banker.JS.Agent

- size: 3.5 KB
- spread via email attachments
- also found on home routers

Source: Kaspersky Security Bulletin 2015

Users attacked: stats



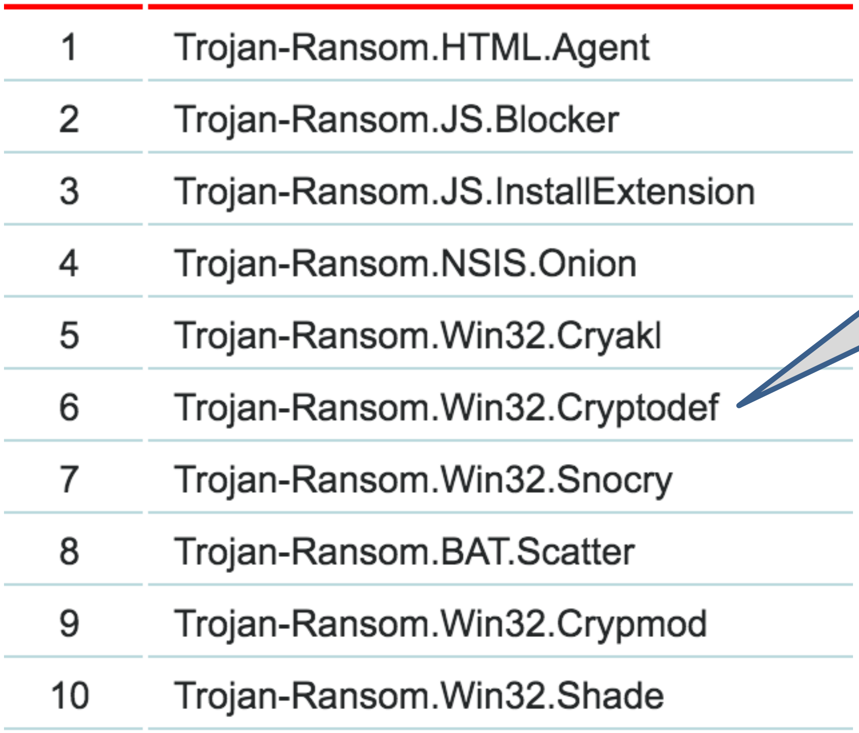


≈ 300,000 users worldwide

A worldwide problem

Source: Kaspersky Security Bulletin 2015

Why own machines: 3. **Ransomware**



1	Trojan-Ransom.HTML.Agent
2	Trojan-Ransom.JS.Blocker
3	Trojan-Ransom.JS.InstallExtension
4	Trojan-Ransom.NSIS.Onion
5	Trojan-Ransom.Win32.Cryakl
6	Trojan-Ransom.Win32.Cryptodef
7	Trojan-Ransom.Win32.Snocry
8	Trojan-Ransom.BAT.Scatter
9	Trojan-Ransom.Win32.Crypmod
10	Trojan-Ransom.Win32.Shade

CryptoWall (2014-)

- targets Windows
- spread by spam emails

≈ 200,000 machines in 2015

A worldwide problem.

Why own machines:
4. Spread to isolated systems

Example: **Stuxtnet**

Windows infection ⇒

Siemens PCS 7 SCADA control software on Windows ⇒

Siemens device controller on isolated network

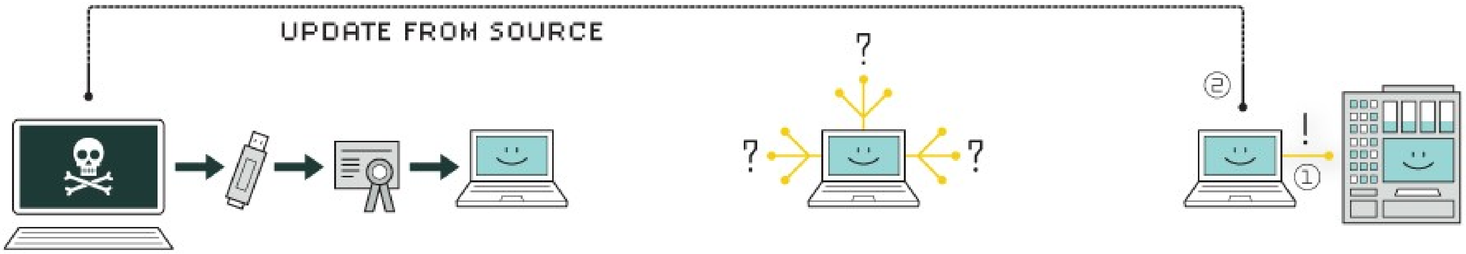
More on this later in course

Example: Mpack

- PHP-based tools installed on compromised web sites
  - Embedded as an iframe on infected page
  - Infects browsers that visit site
- Features
  - management console provides stats on infection rates
  - Sold for several 100$
  - Customer care can be purchased, one-year support contract
- Impact: 500,000 infected sites (compromised via SQL injection)
  - Several defenses: e.g. Google safe browsing

Cyber War

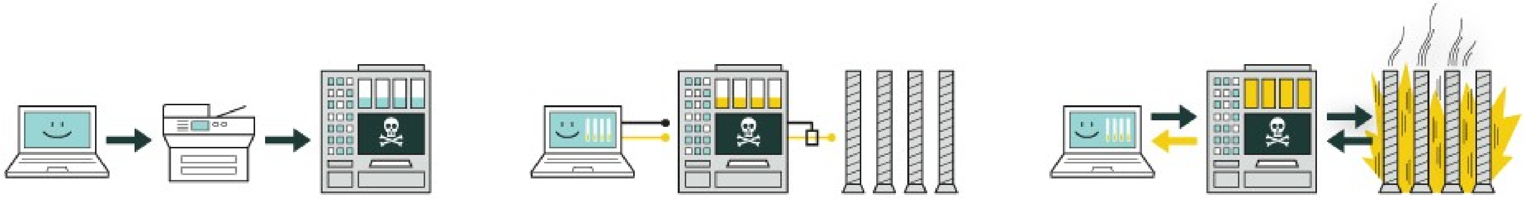
HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

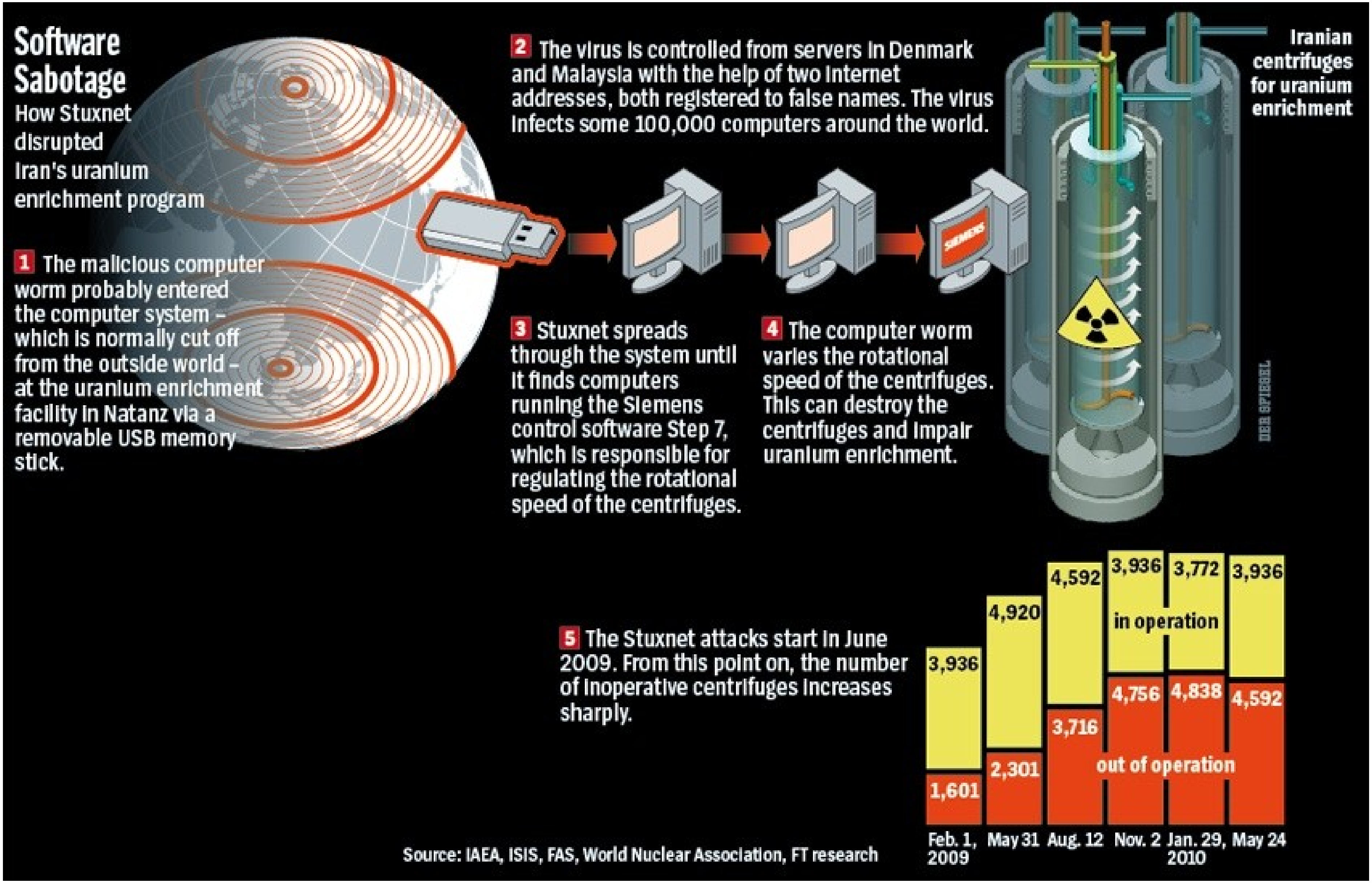
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

Iranian centrifuges for uranium enrichment

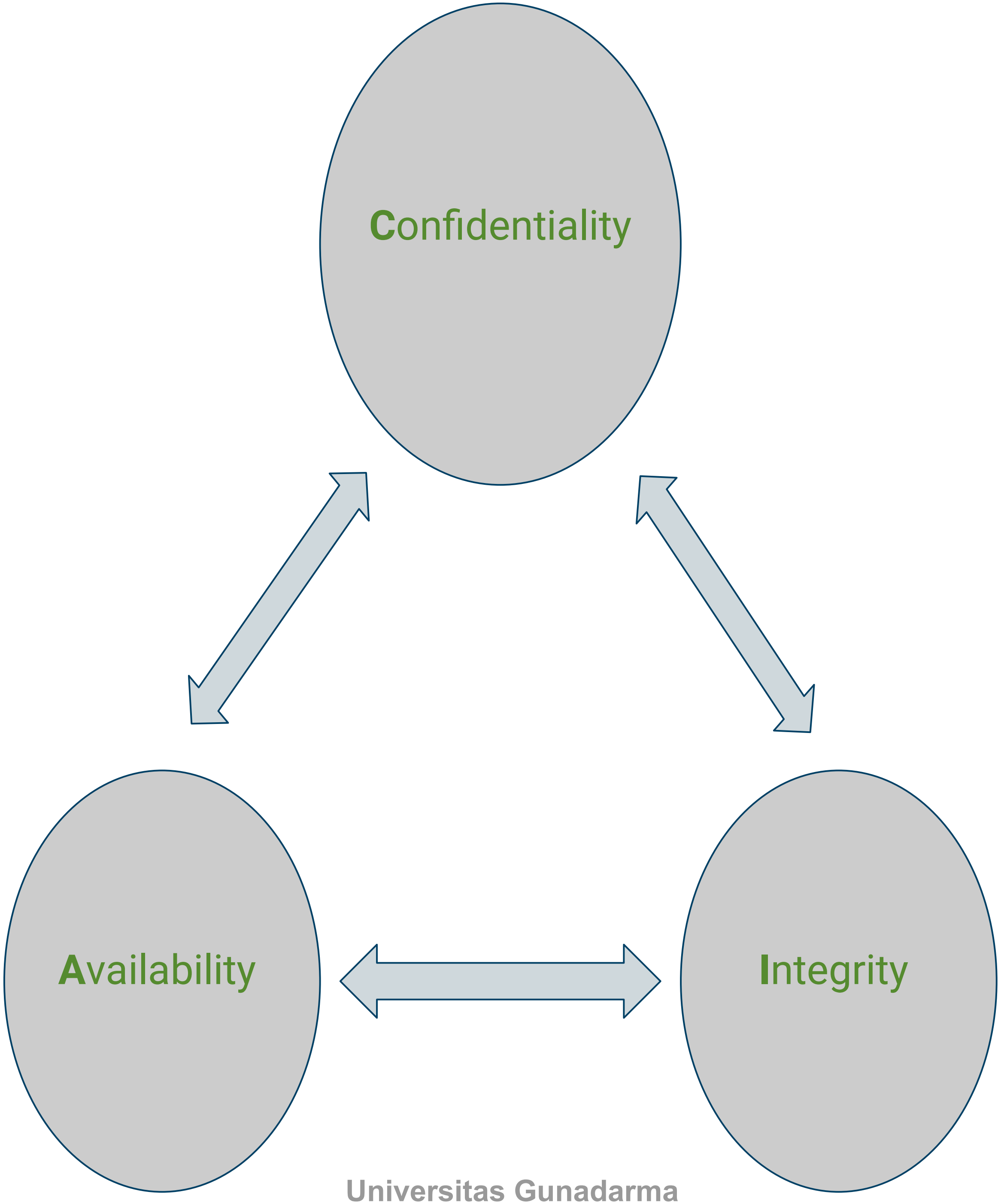
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Security Components

Security Components

- **Confidentiality**: Need access control, Cryptography, Existence of data
- **Integrity**: No change, content, source, prevention mechanisms, detection mechanisms
- **Availability**: Denial of service attacks
- **A**=Availability, Authenticity or Accountability
- Confidentiality, Integrity and Availability (CIA)


Confidentiality
Availability
Integrity

Step in Cracking Information

- **Information Gathering**: Public sources/tools.
- **Port Scanning**: Find open TCP ports.
- **Network Enumeration**: Map the network. Servers and workstations. Routers, switches, firewalls.
- **Gaining Access**: Keeping root/administrator access
- **Modifying**: Using access and modifying information
- **Leaving a backdoor**: To return at a later date.
- **Covering tracks**

Types of Malwares

- **Viruses**: Code that attaches itself to programs, disks, or memory to propagate itself.
- **Worms**: Installs copies of itself on other machines on a network, e.g., by finding user names and passwords
- **Trojan horses**: Pretend to be a utility. Convince users to install on PC.
- **Rootkit**: Gets “root” (admin) privilege

Types of Malwares

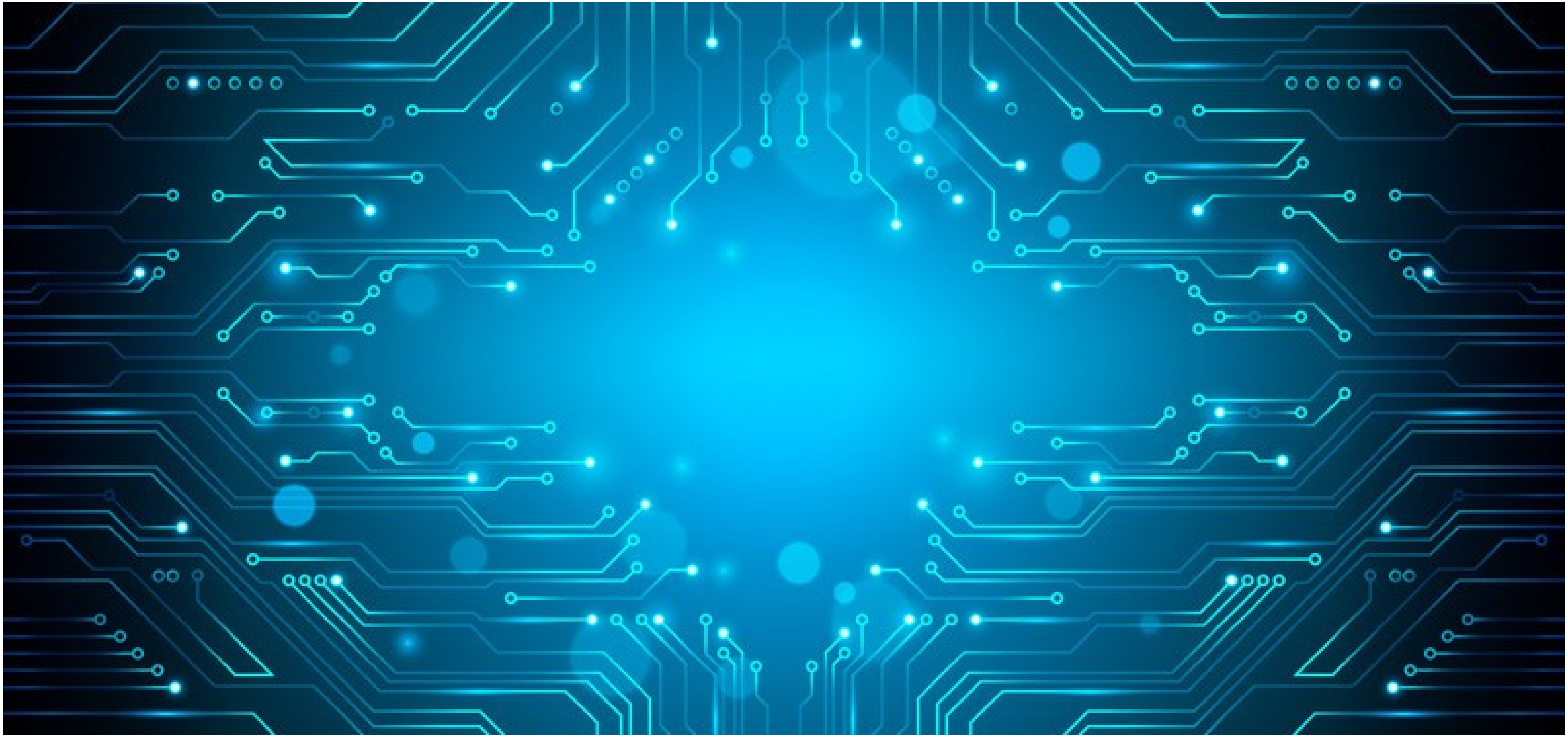
- **Spyware**: Collect information. Legally used by employers.
- **Key Loggers**
- **Hoax**: Use emotion to propagate, e.g., child's last wish.
- **Trap Door**: Undocumented entry point for debugging purposes
- **Logic Bomb**: Instructions that trigger on some event in the future
- **Zombie**: Malicious instructions that can be triggered remotely. The attacks seem to come from other victims.

Types Of Attacks

- **Malware**
- **Security Breach**: unauthorized access
- **Denial of Service (DoS)**: Flooding with traffic/requests
- **Web attack**: SQL injection
- **Cross-Site Scripting**: Direct users to malicious sites using SQL injection
- **Session Hijacking**: Taking over an active session
- **DNS Poisoning**: Direct users to malicious sites
- **Brute Force**: Try all passwords.
- **Port Scanning** ⇒ Disable unnecessary services and close ports
- **Network Mapping**

Types Of Attacks

- **Cyber Stalking**: Harassing/threatening using Internet
- **Cyber Frauds**: Nigerian official wants to deposit large funds into your bank account
- **Identity Theft**: Get credit cards using your Social Security number
- **Phishing**: Email claiming to be from bank/employer/government



Data Growing

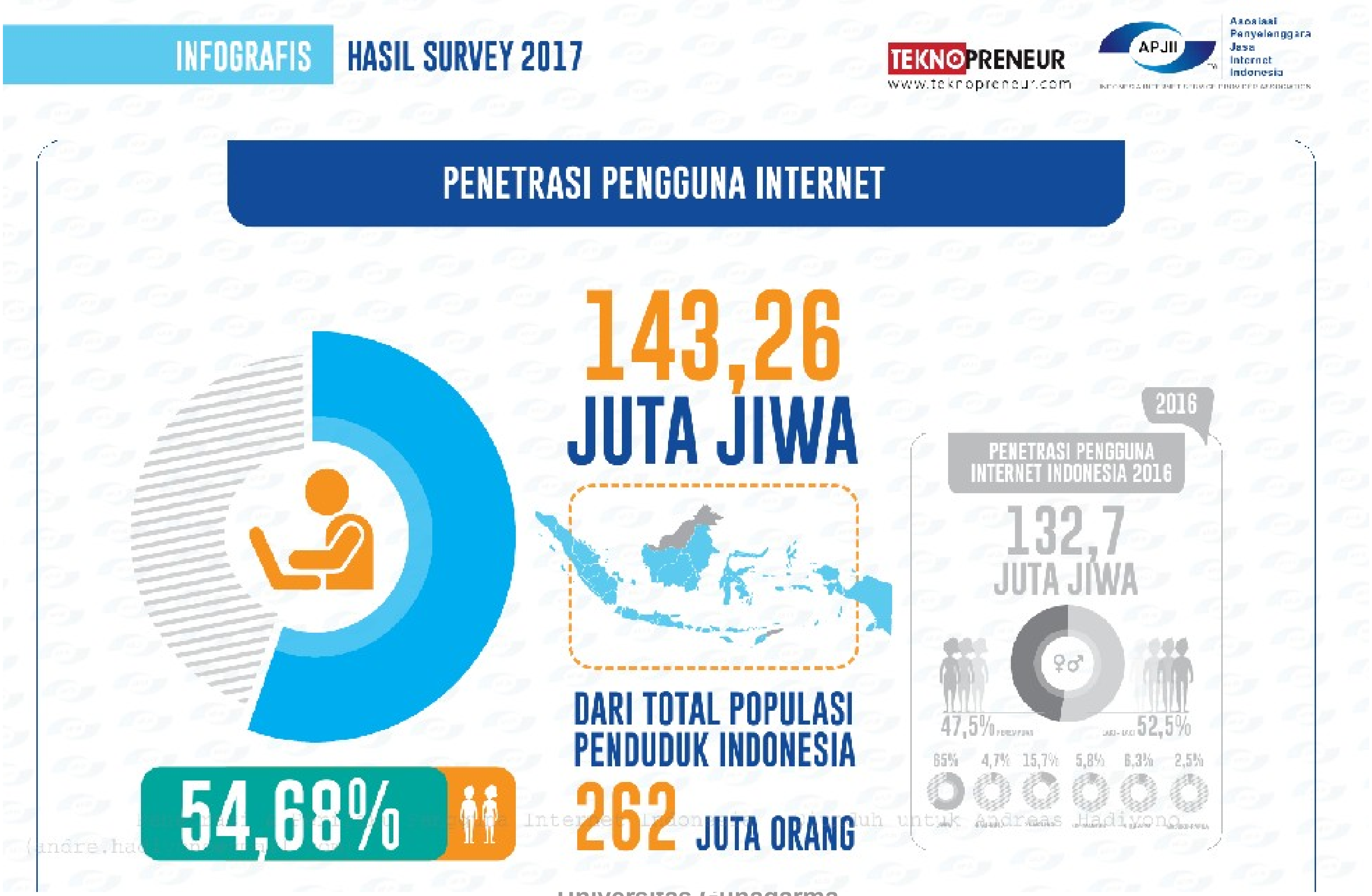
Universitas Gunadarma

Sistem Keamanan Komputer

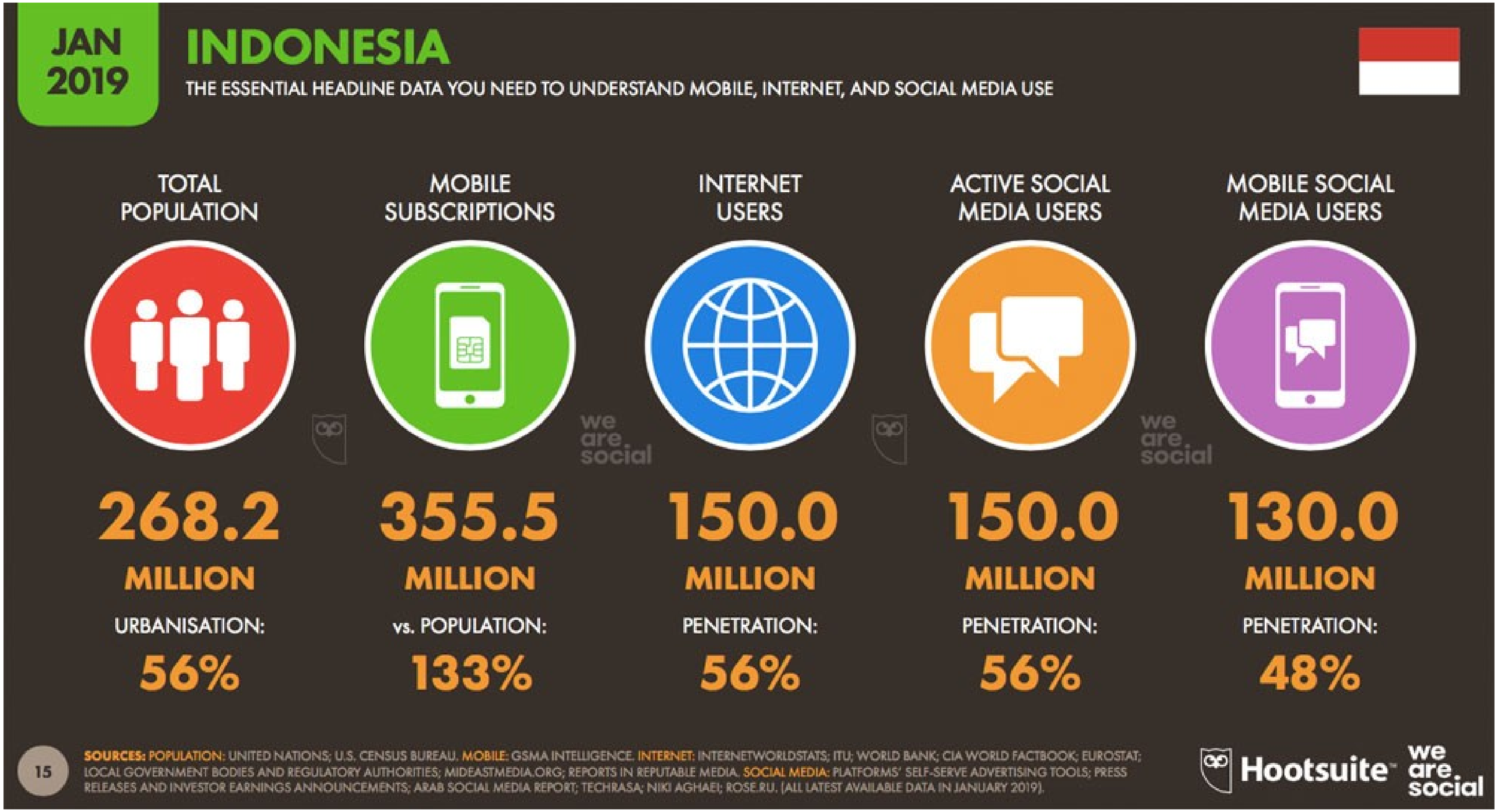
Data All Around

- Lots of data is being collected and warehouse
  - Web data, e-commerce
  - Financial Transactions, bank/credit transaction
  - Online trading, purchasing
  - Healthcare
  - Social network
  - etc
- Increasing technology telecomunication

Internet users in Indonesia



Network Subscription



JAN 2019

INDONESIA

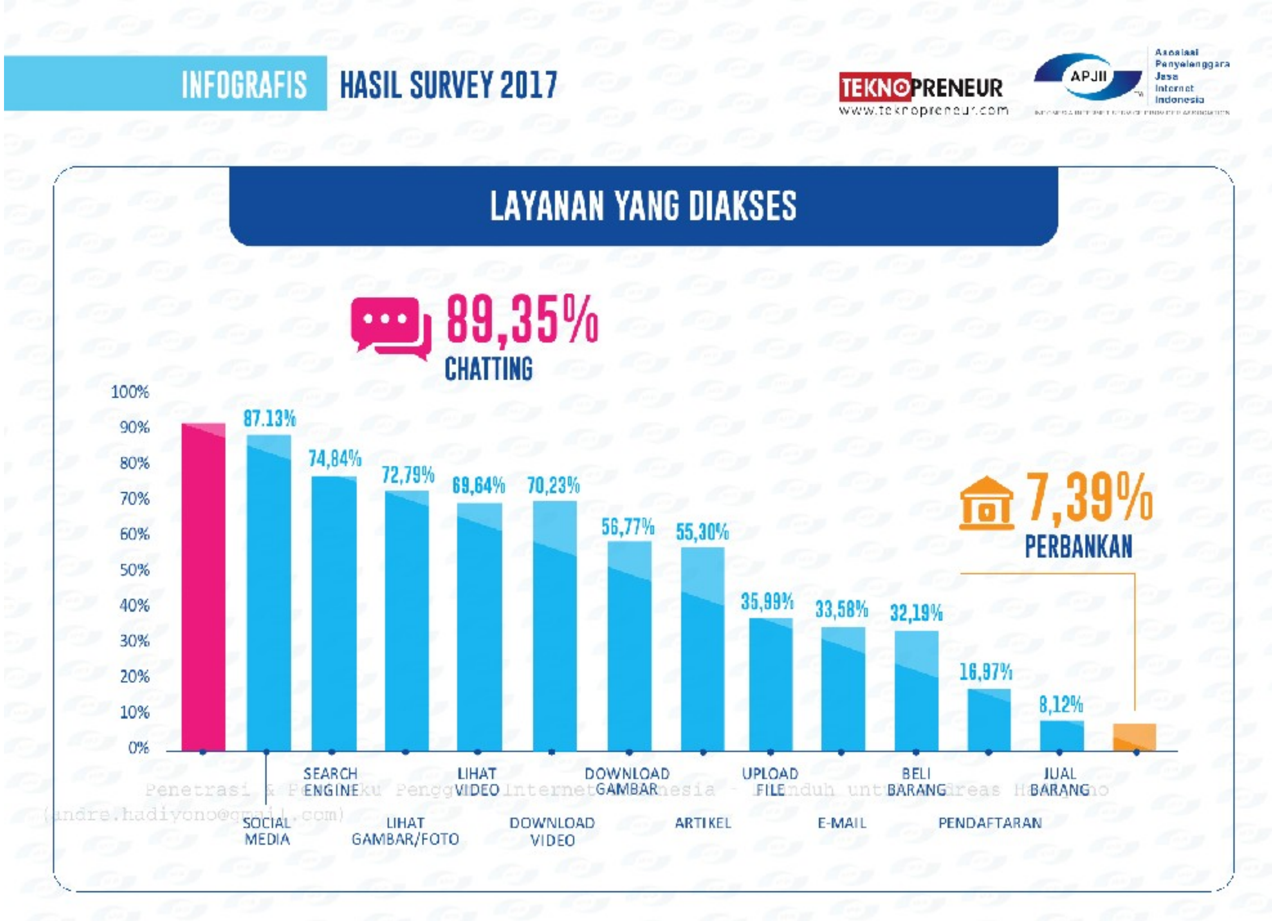
THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL POPULATION	MOBILE SUBSCRIPTIONS	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	MOBILE SOCIAL MEDIA USERS
268.2 MILLION	355.5 MILLION	150.0 MILLION	150.0 MILLION	130.0 MILLION
URBANISATION:	vs. POPULATION:	PENETRATION:	PENETRATION:	PENETRATION:
56%	133%	56%	56%	48%

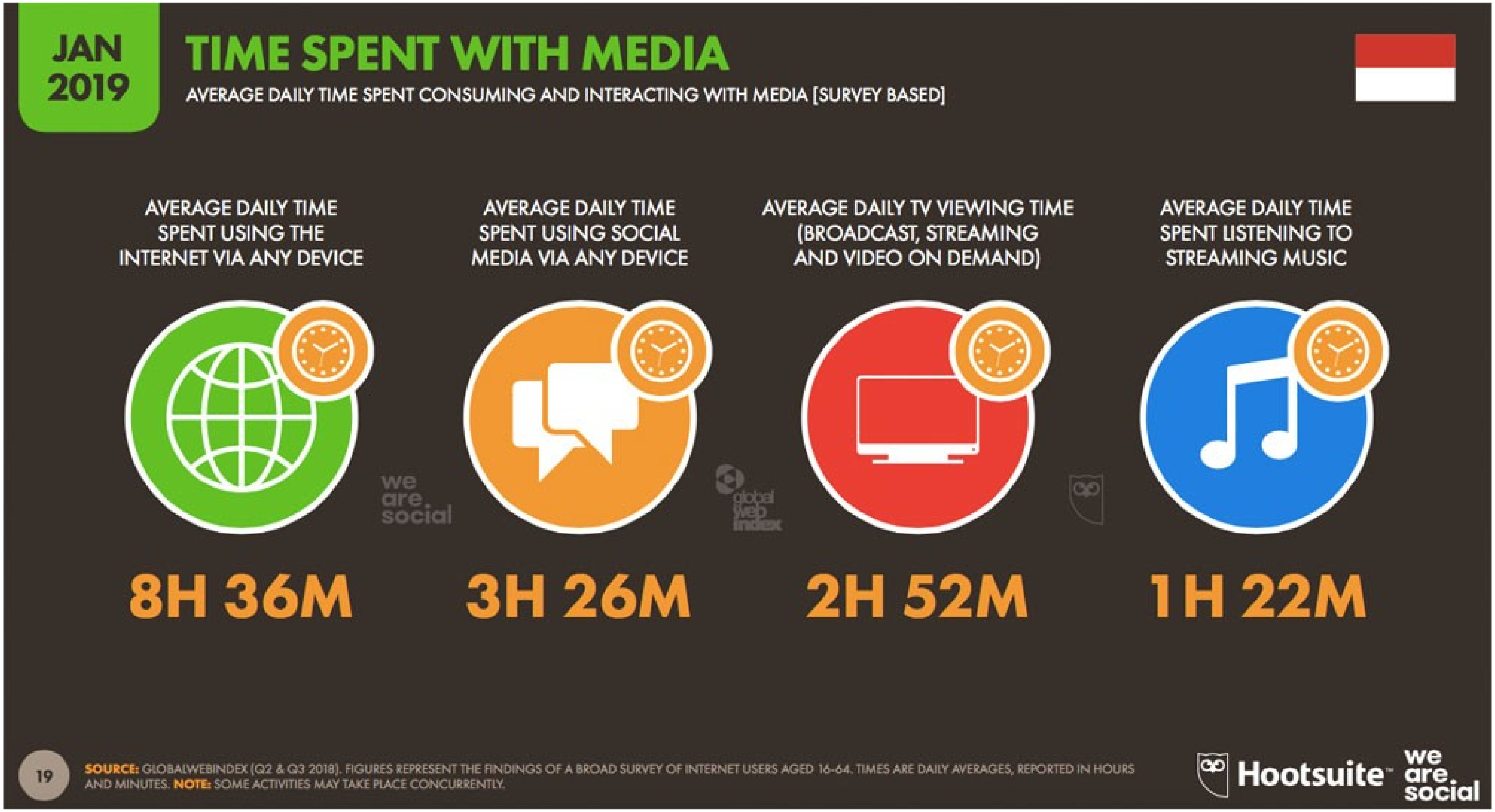
15 SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU. MOBILE: GSMA INTELLIGENCE. INTERNET: INTERNETWORLDSTATS; ITU; WORLD BANK; CIA WORLD FACTBOOK; EUROSTAT; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; MIDEASTMEDIA.ORG; REPORTS IN REPUTABLE MEDIA. SOCIAL MEDIA: PLATFORMS' SELF-SERVE ADVERTISING TOOLS; PRESS RELEASES AND INVESTOR EARNINGS ANNOUNCEMENTS; ARAB SOCIAL MEDIA REPORT; TECHRASA; NIKI AGHAEI; ROSE.RU. (ALL LATEST AVAILABLE DATA IN JANUARY 2019).

Hootsuite we are social

Information Statistic



Time Spend



JAN 2019

TIME SPENT WITH MEDIA

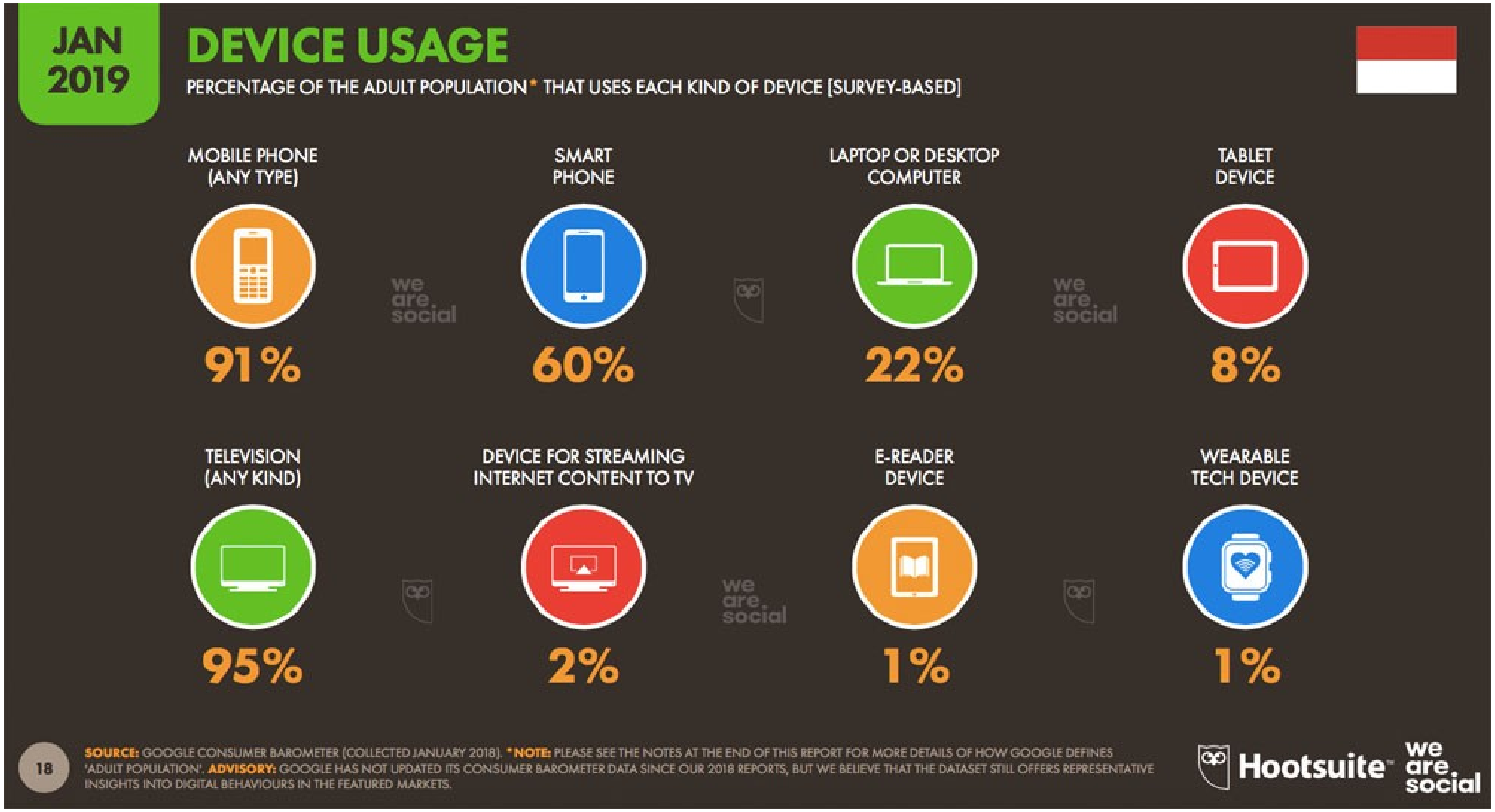
AVERAGE DAILY TIME SPENT CONSUMING AND INTERACTING WITH MEDIA [SURVEY BASED]

AVERAGE DAILY TIME SPENT USING THE INTERNET VIA ANY DEVICE	AVERAGE DAILY TIME SPENT USING SOCIAL MEDIA VIA ANY DEVICE	AVERAGE DAILY TV VIEWING TIME (BROADCAST, STREAMING AND VIDEO ON DEMAND)	AVERAGE DAILY TIME SPENT LISTENING TO STREAMING MUSIC
8H 36M	3H 26M	2H 52M	1H 22M

19 **SOURCE:** GLOBALWEBINDEX (Q2 & Q3 2018). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16-64. TIMES ARE DAILY AVERAGES, REPORTED IN HOURS AND MINUTES. **NOTE:** SOME ACTIVITIES MAY TAKE PLACE CONCURRENTLY.

Hootsuite we are social

Device Usage



JAN 2019

DEVICE USAGE

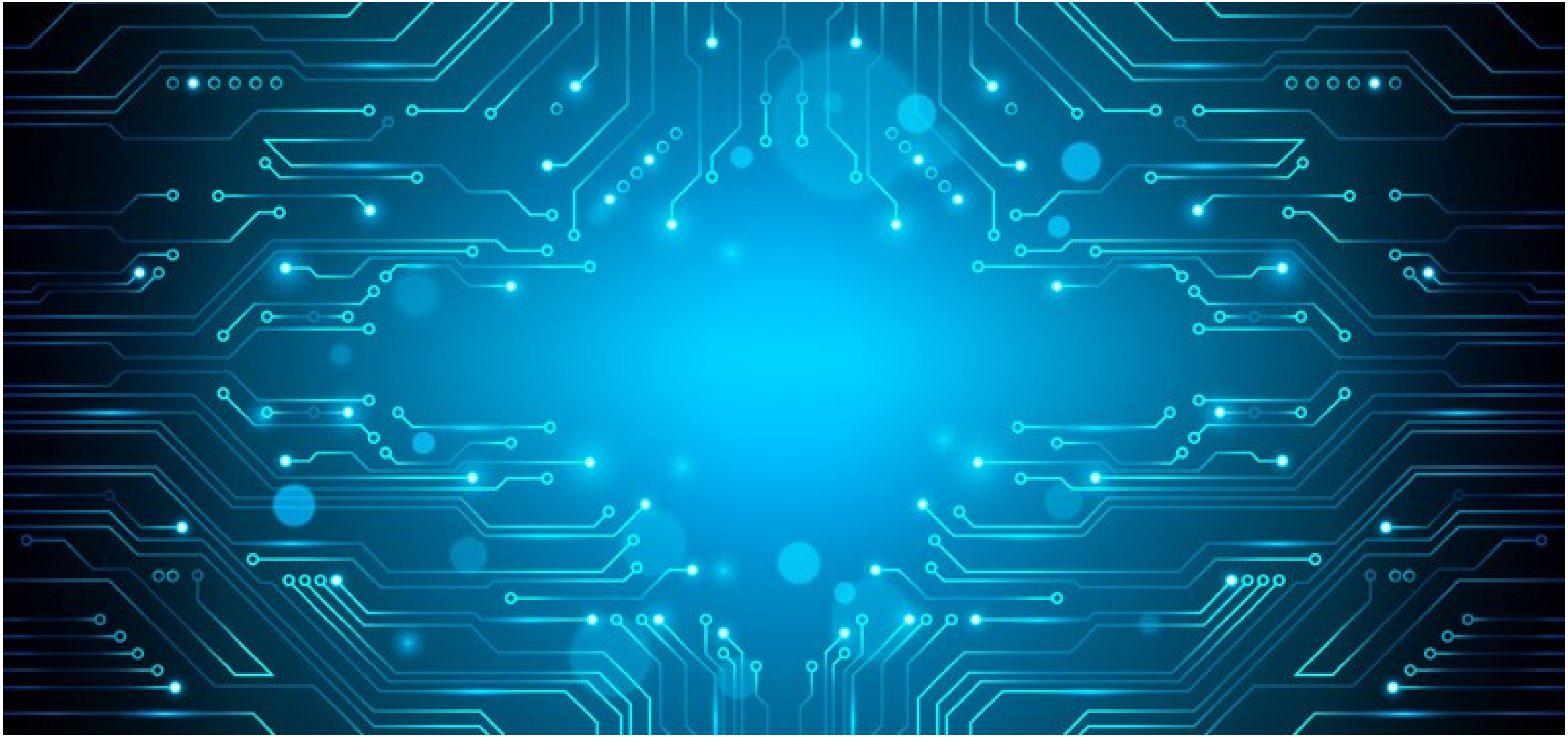
PERCENTAGE OF THE ADULT POPULATION* THAT USES EACH KIND OF DEVICE [SURVEY-BASED]

MOBILE PHONE (ANY TYPE)	SMART PHONE	LAPTOP OR DESKTOP COMPUTER	TABLET DEVICE
91%	60%	22%	8%

TELEVISION (ANY KIND)	DEVICE FOR STREAMING INTERNET CONTENT TO TV	E-READER DEVICE	WEARABLE TECH DEVICE
95%	2%	1%	1%

18

SOURCE: GOOGLE CONSUMER BAROMETER (COLLECTED JANUARY 2018). ***NOTE:** PLEASE SEE THE NOTES AT THE END OF THIS REPORT FOR MORE DETAILS OF HOW GOOGLE DEFINES 'ADULT POPULATION'. **ADVISORY:** GOOGLE HAS NOT UPDATED ITS CONSUMER BAROMETER DATA SINCE OUR 2018 REPORTS, BUT WE BELIEVE THAT THE DATASET STILL OFFERS REPRESENTATIVE INSIGHTS INTO DIGITAL BEHAVIOURS IN THE FEATURED MARKETS.



Big Data

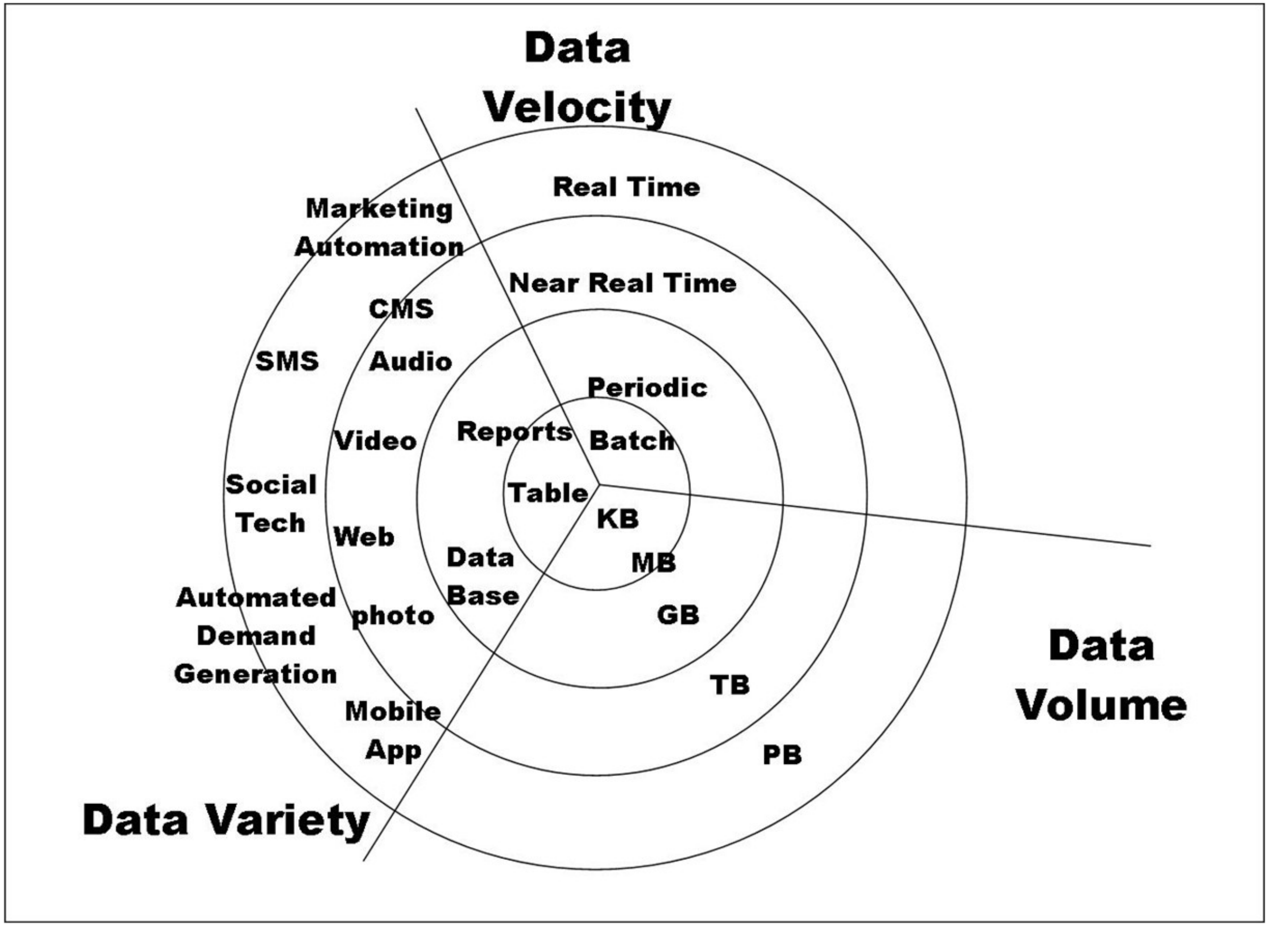
Universitas Gunadarma

Sistem Keamanan Komputer

Big Data

- Big Data is any data that is expensive to manage and hard to extract value from
  - Volume
    - The size of the data
  - Velocity
    - The latency of data processing relative to the growing demand for interactivity
  - Variety and Complexity
    - The diversity of sources, formats, quality, structures.

Big Data

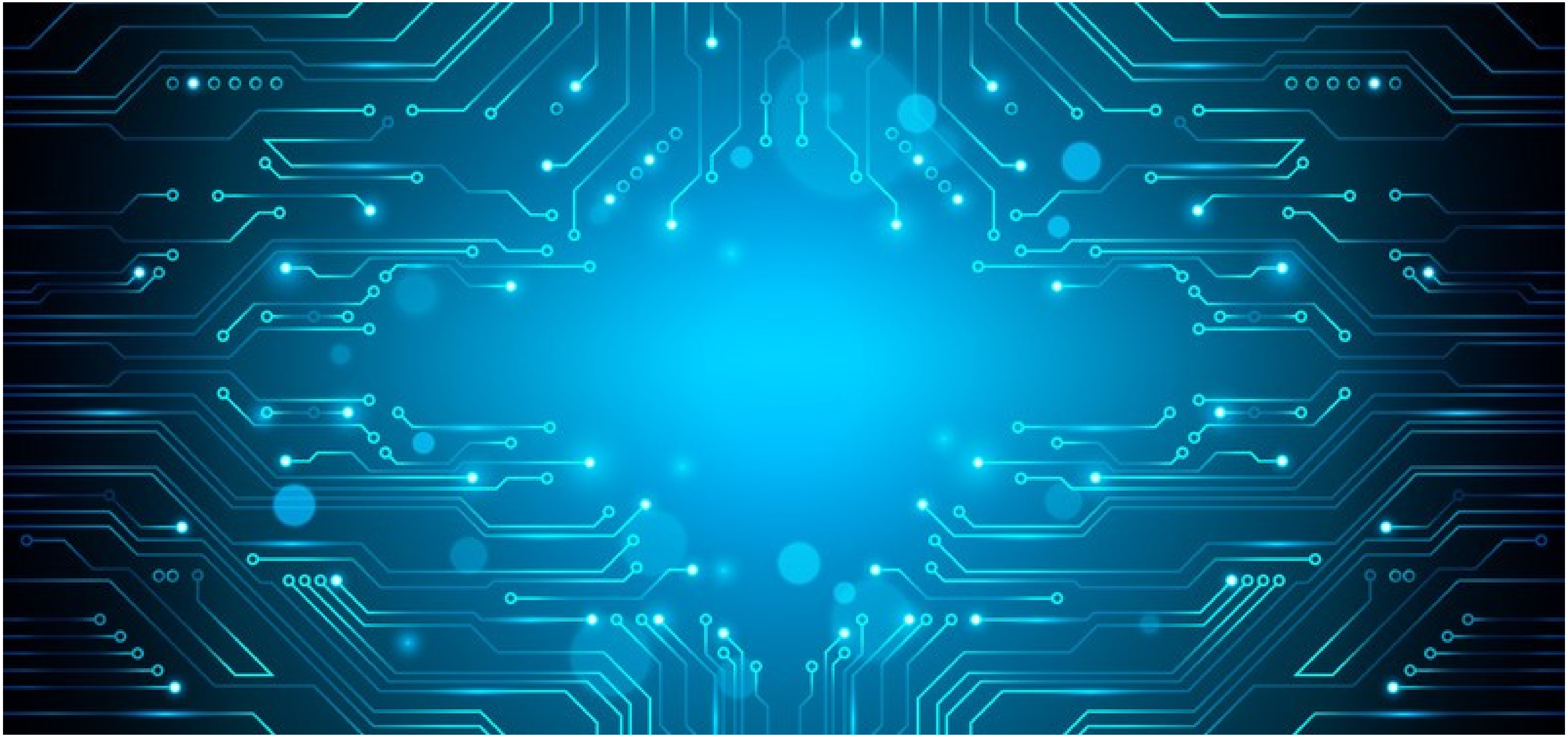

Data
Velocity
Real Time
Near Real Time
Periodic
Batch
Marketing
Automation
CMS
SMS
Audio
Video
Reports
Social
Tech
Table
Web
KB
Data
Base
MB
Automated
Demand
Generation
photo
GB
TB
Mobile
App
PB
Data
Volume
Data Variety

Type of Data

- Relational Data (Tables/Transaction/Legacy Data)
- Text Data (Web)
- Semi-structured Data (XML)
- Graph Data
- Social Network, Semantic Web (RDF), …
- Streaming Data
- etc

Collecting data

- Aggregation and Statistics
  - Data warehousing and OLAP
- Indexing, Searching, and Querying
  - Keyword based search
  - Pattern matching (XML/RDF)
- Knowledge discovery
  - Data Mining
  - Statistical Modeling
- etc



Big Data

Universitas Gunadarma

Sistem Keamanan Komputer

thank you
рахмат
danke
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
спасибо
mersi
kia ora
barka
welalin
tack
spas
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
mahalo
tapadh leat
gracias
хвала
asante
manana
obrigada
tenki
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
bedankt
bayarlalaa
gràcie
hvala
enkosi
dziękuję
akun
dankon
aćiū
djiere dieuf
tau
mochchakkeram
murakoze
chokrane
дякую
mamnun
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dėkuji
obrigado
mèsi
didi madloba
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
ありがとう
najis tuke
kam sah hamnida
rahmat
terima kasih
tanemirt
rahmet
grazie
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercê
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci