Cybersecurity by the #s

Regulatory Internet Governance Symposium – Vanuatu

20 October 2016

APNIC

Cybersecurity by the #s

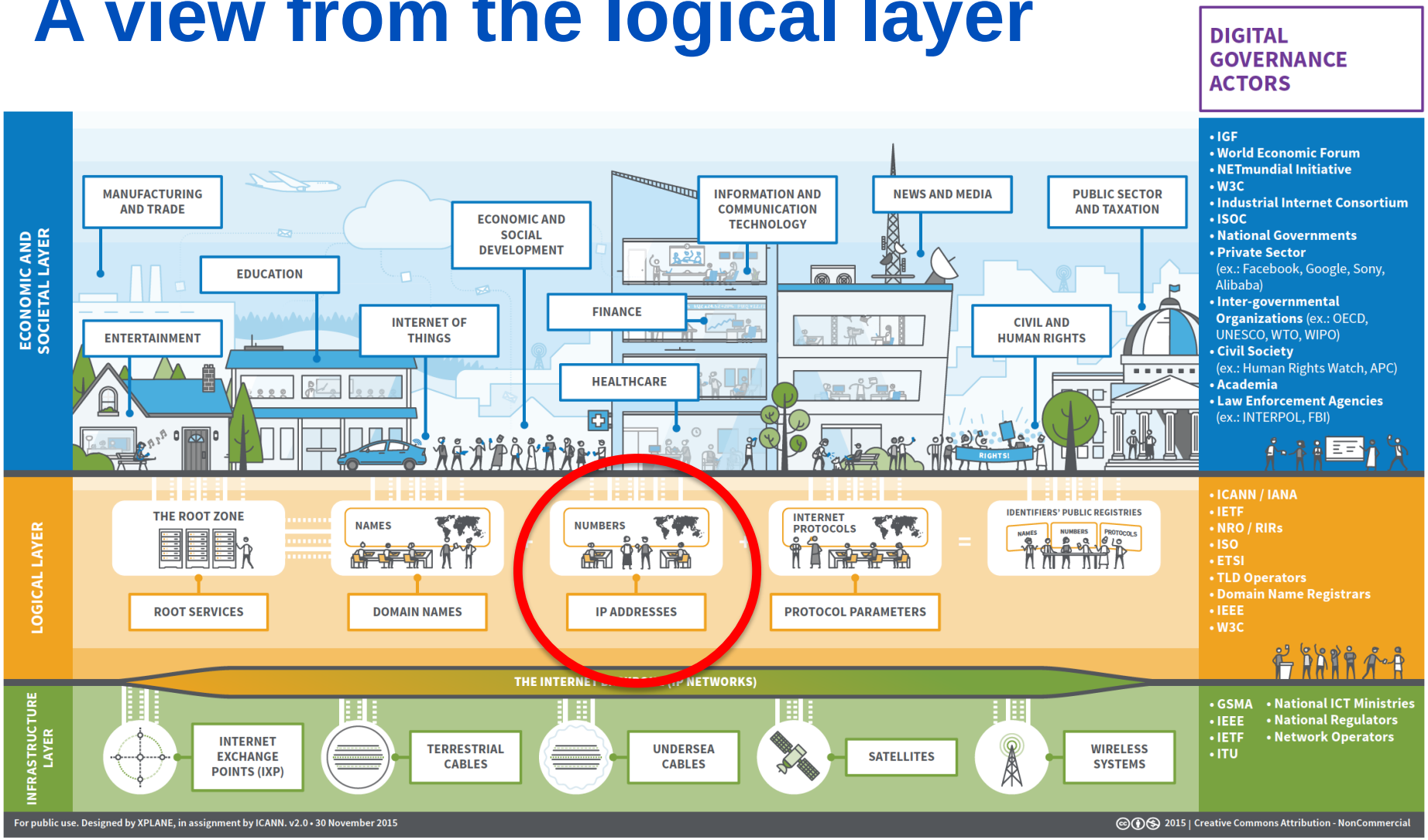
Network Security

- A view from the logical layer
- Network Security
- What are we up against?
- The cybersecurity ecosystem

CERT | CSIRT

- Incident Response
- Coordination
- Information Sharing
- Building a CERT
- Components of a CERT/CSIRT
- The Road Forward

A view from the logical layer

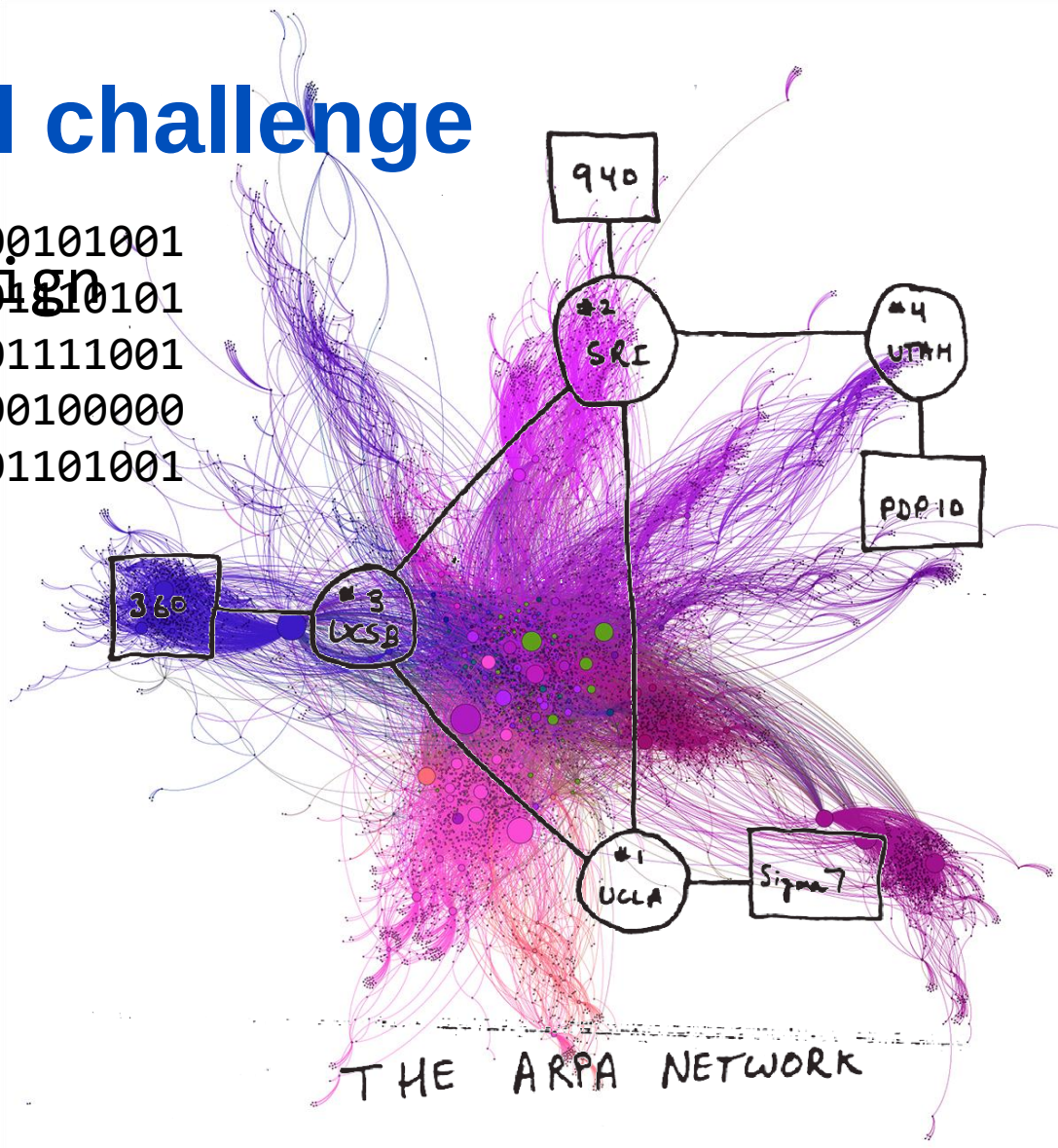


https://www.icann.org/news/multimedia/1563

The fundamental challenge

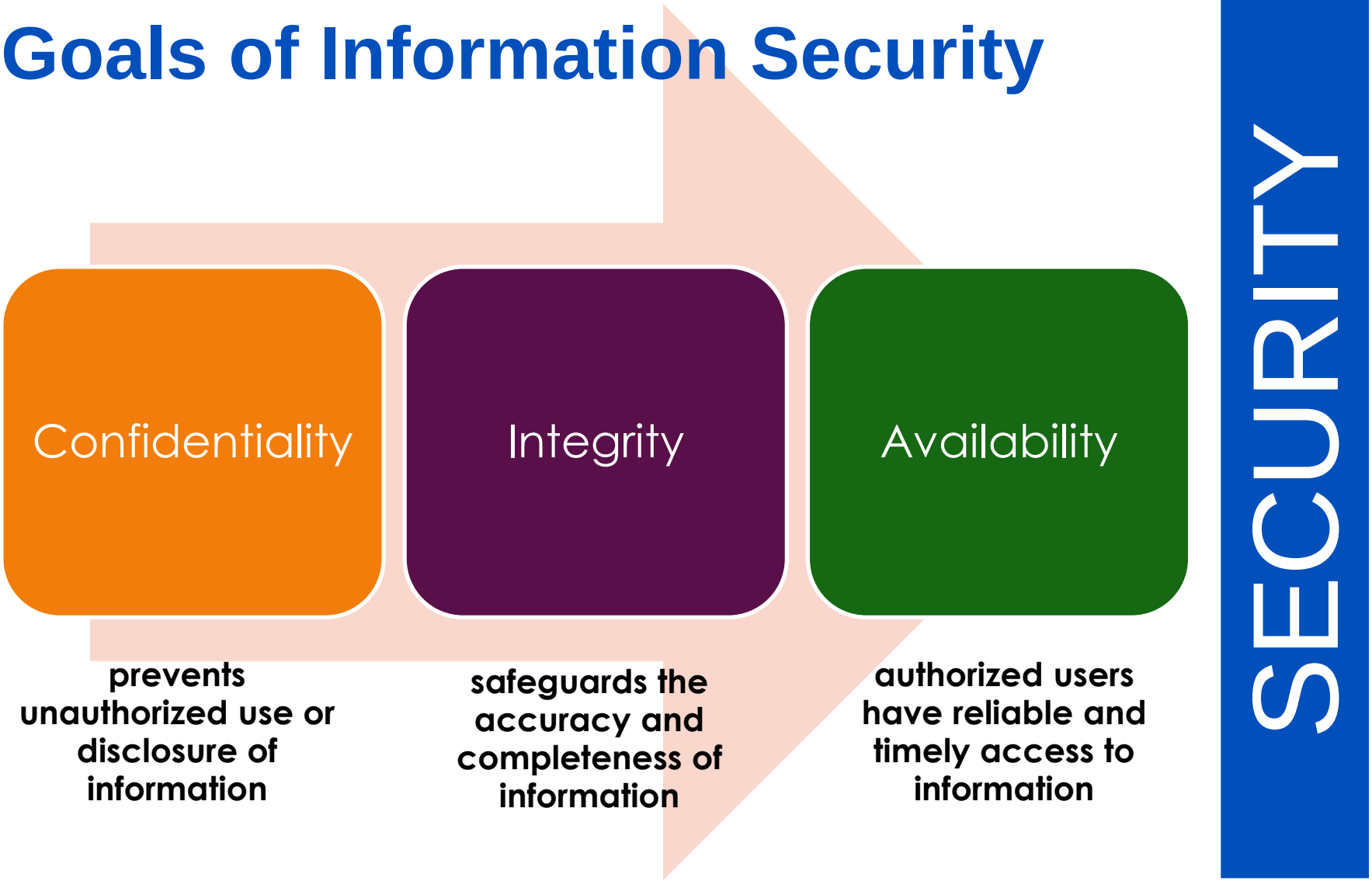
(in)Security by Design

```
00101000 01101001 01101110 00101001
01110011 01100101 01100011 01101101
01110010 01101001 01110100 01111001
00100000 01100010 01111001 00100000
01100100 01100101 01110011 01101001
01100111 01101110
```



https://blog.apnic.net/2015/07/07/mapping-the-internet-in-the-asia-pacific/

Goals of Information Security



Terms: Breaking it down

- **Threat**
  - Any circumstance or factor with the potential to cause harm
  - *a motivated, capable adversary*
- **Vulnerability**
  - A weakness in a system; in procedures, design, or implementation that can be exploited
    - Software bugs, design flaws, operational mistakes
- **Risk** = likelihood x consequences
  - The probability that a particular vulnerability will occur
  - The severity (impact) of that occurrence

Security tradeoffs

- Services offered vs. security provided
  - Each service offers its own security risk
  - The more services, the less security
- Ease of use vs. security
  - Every security mechanism causes inconvenience
  - The more “plug n play”, the less security
- Risk of loss vs. Cost of security
  - Assets carry value and risk of loss
  - The higher the value, the higher the security cost
- These factors can be balanced in a comprehensive security policy

What are we up against?

APNIC

What can the attackers do?

- Eavesdropping – Listen in on communications
- Masquerading – Impersonating someone else
- Forgery – Invent or duplicate/replay information
- Trespass – Obtain unauthorised access
- Subversion – Modify data and messages in transit
- Destruction – Vandalise or delete important data
- Disruption – Disable or prevent access to services
- Infiltration – Hide out inside our machines
- Hijacking – “Own” and use machines for nefarious purposes

And why do they do it?

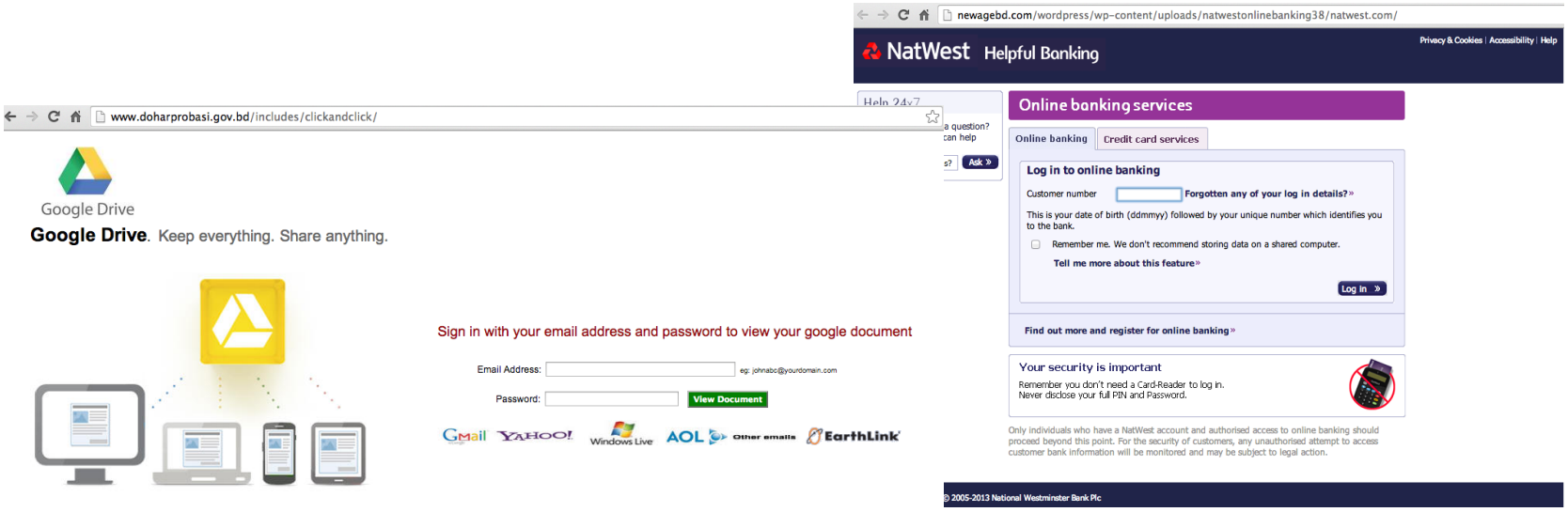
Motivation	Examples
Knowledge driven	• Recreational • Research
Issue-based	• Hacktivism • Patriotism
Antisocial	• Revenge • Vandalism
Competitive	• Theft of IP • Damage to competitors
Criminal	• Theft of assets • Extortion
Strategic	• Espionage • State-driven or sponsored

And, how to they do it?

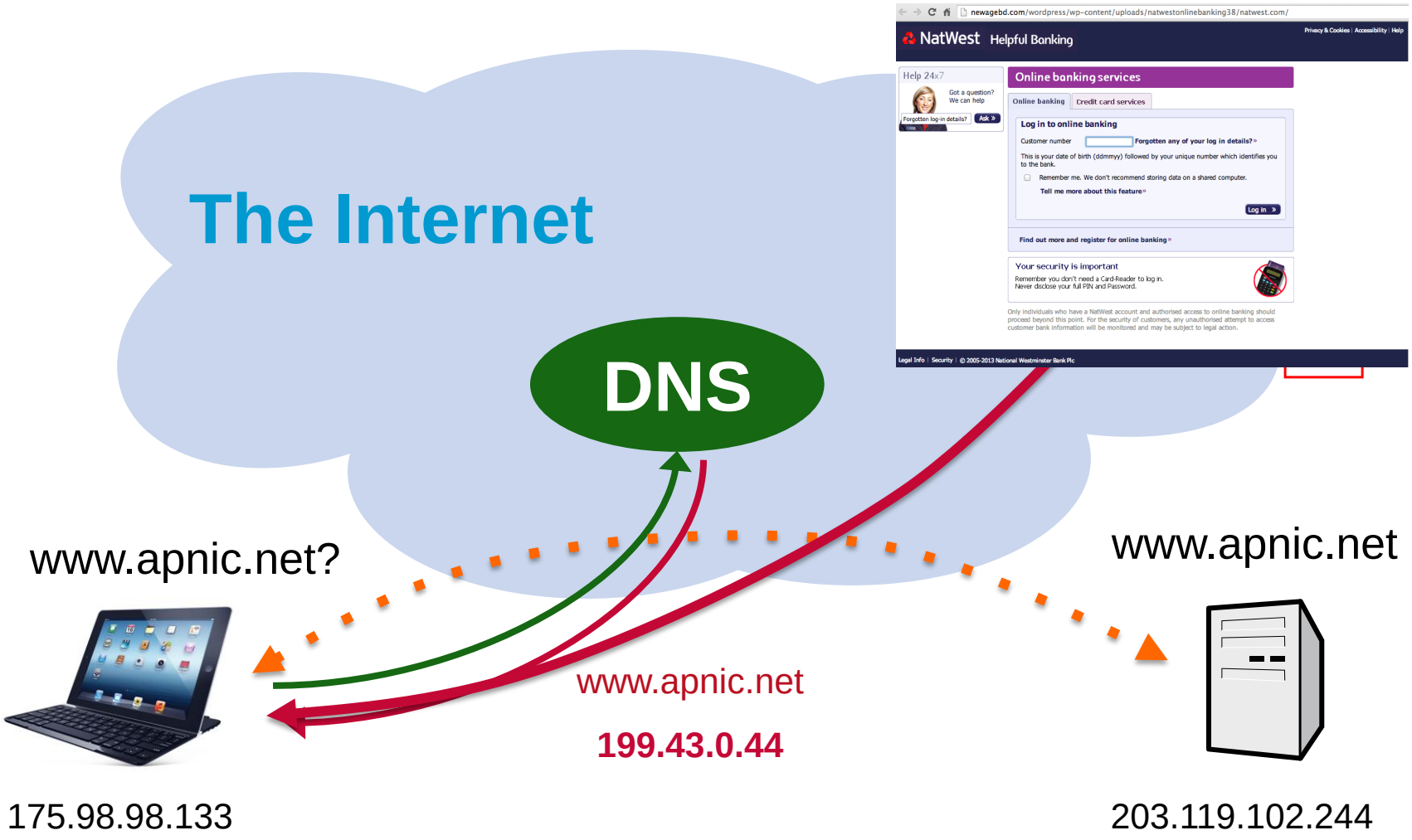
- Targeting the user
  - Masquerading
  - “Phishing”
  - DNS Cache Poisoning
- IP Address “spoofing”
- Disruption
  - DoS attacks
  - DDoS attacks

“Phishing”

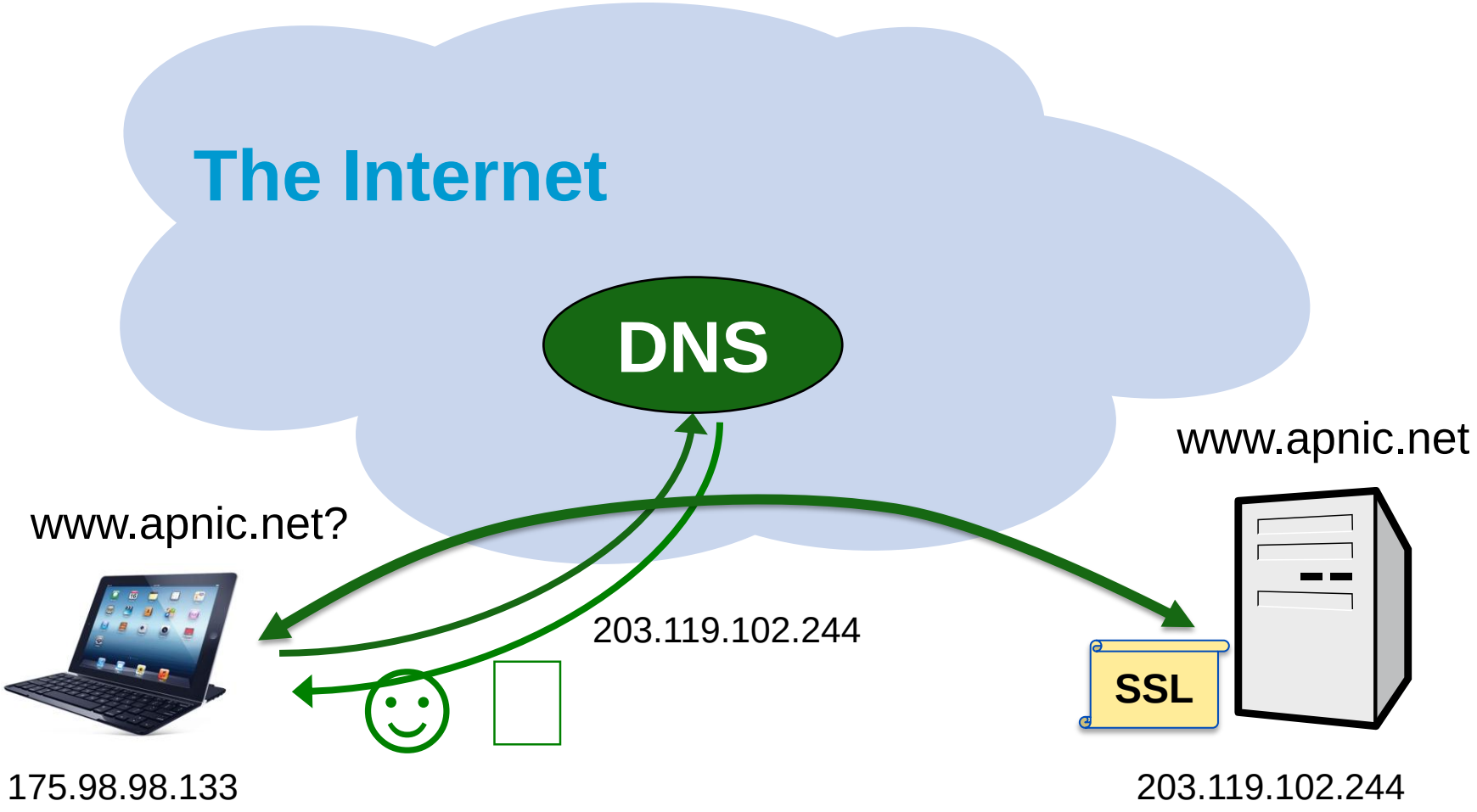
- “Fishing” for information such as usernames, passwords, credit card details, other personal information
- Ex: Forged emails apparently from legitimate enterprises, direct users to forged websites.



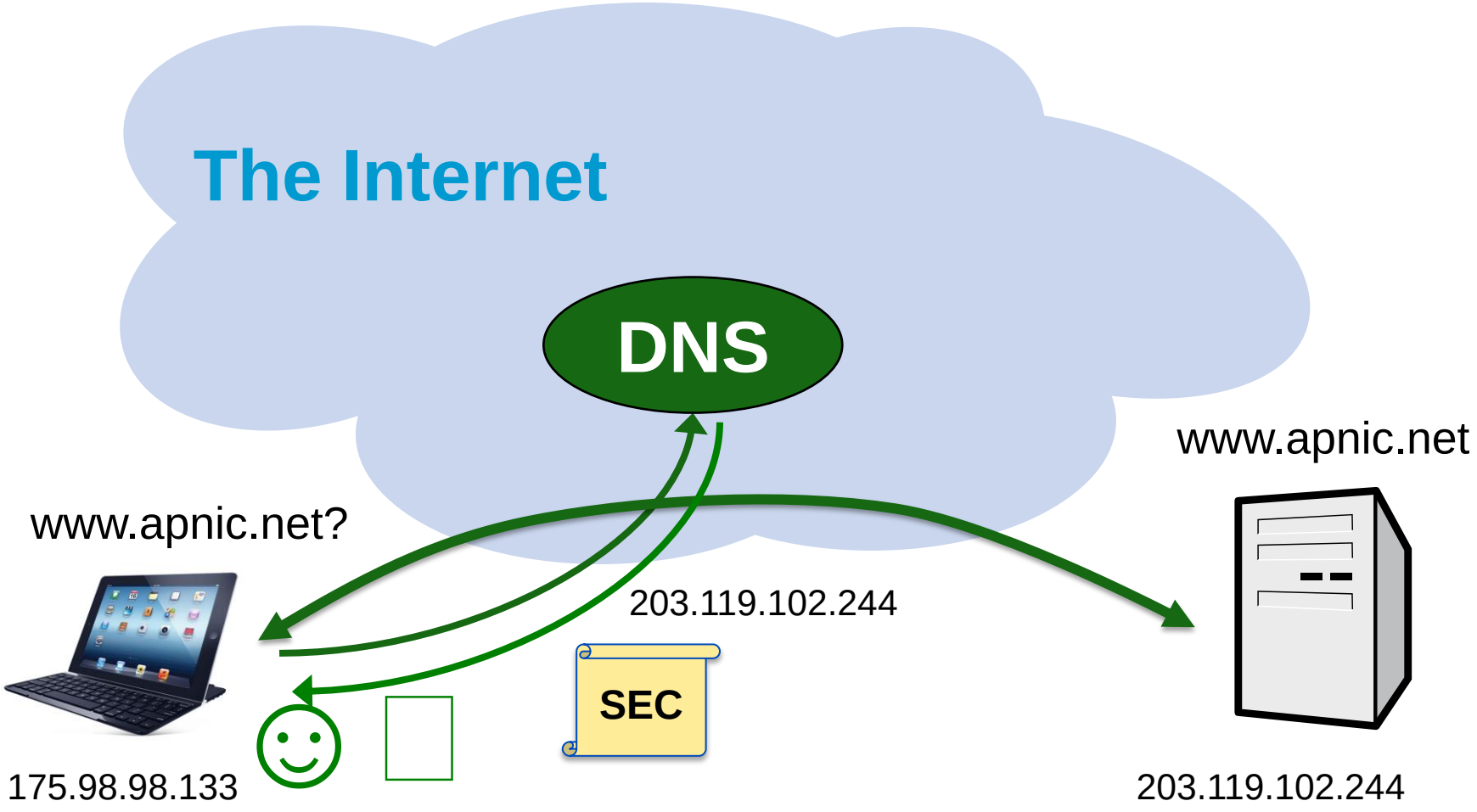
DNS Cache Poisoning



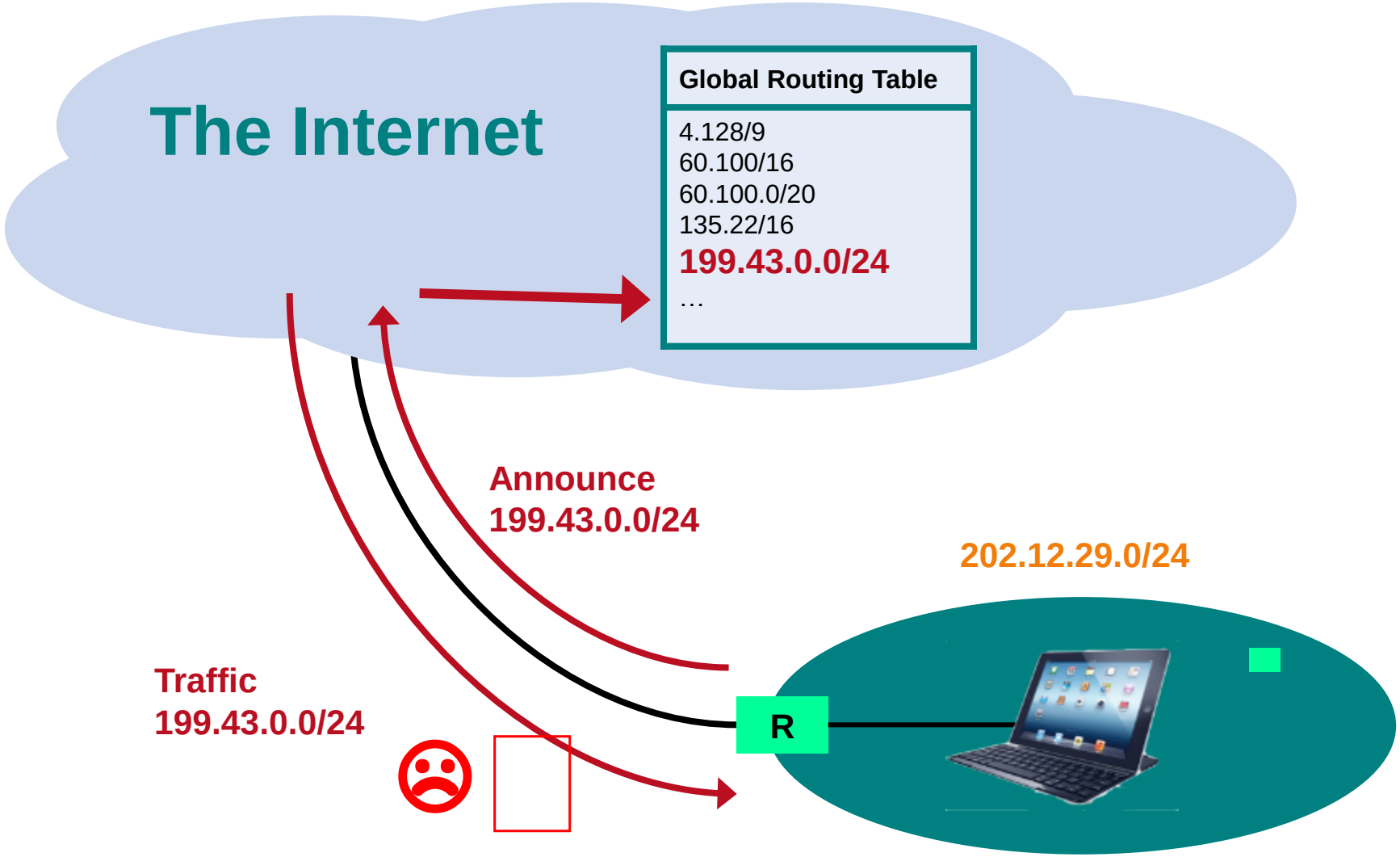
Securing websites – SSL certificates



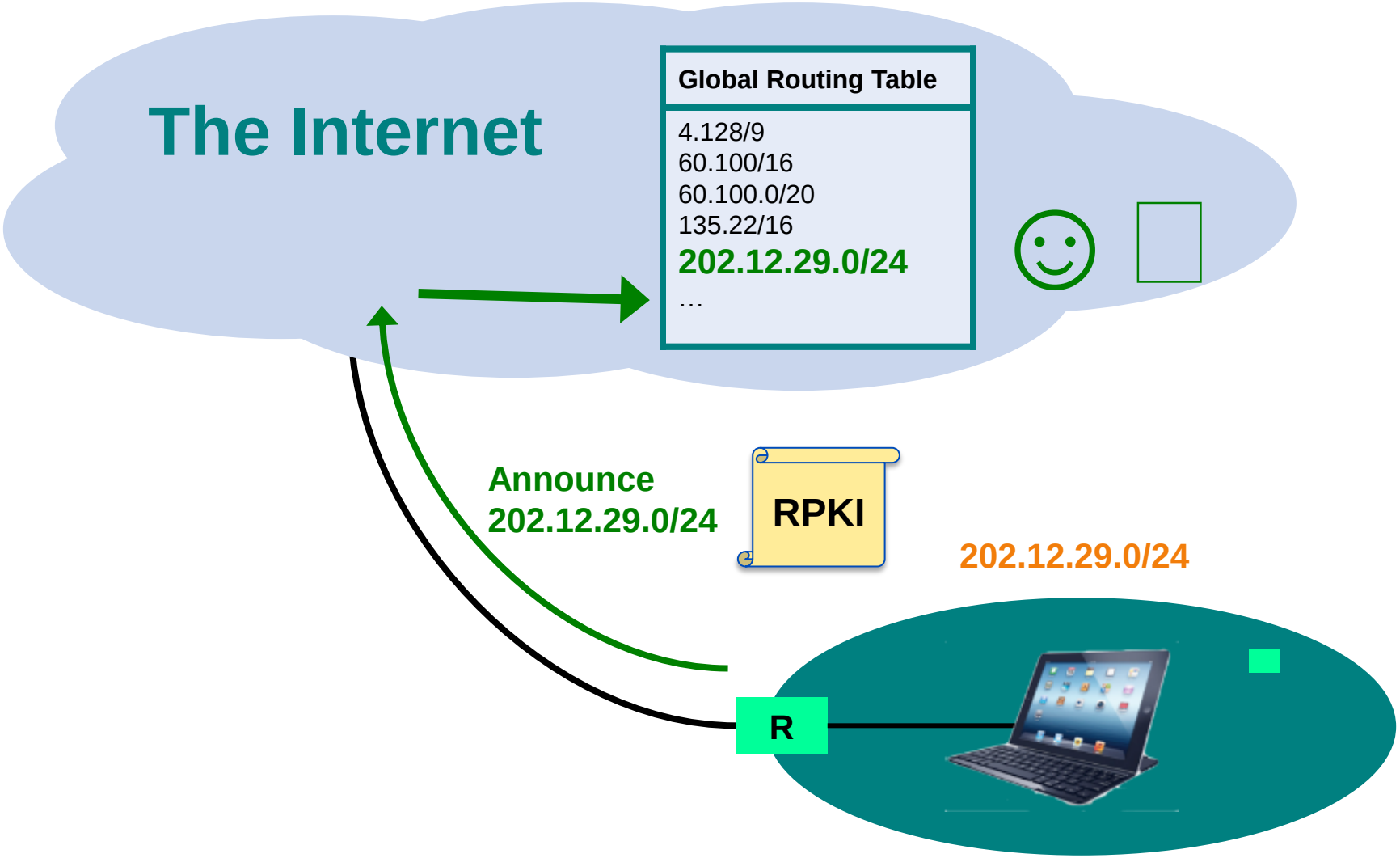
Securing DNS – DNSSEC



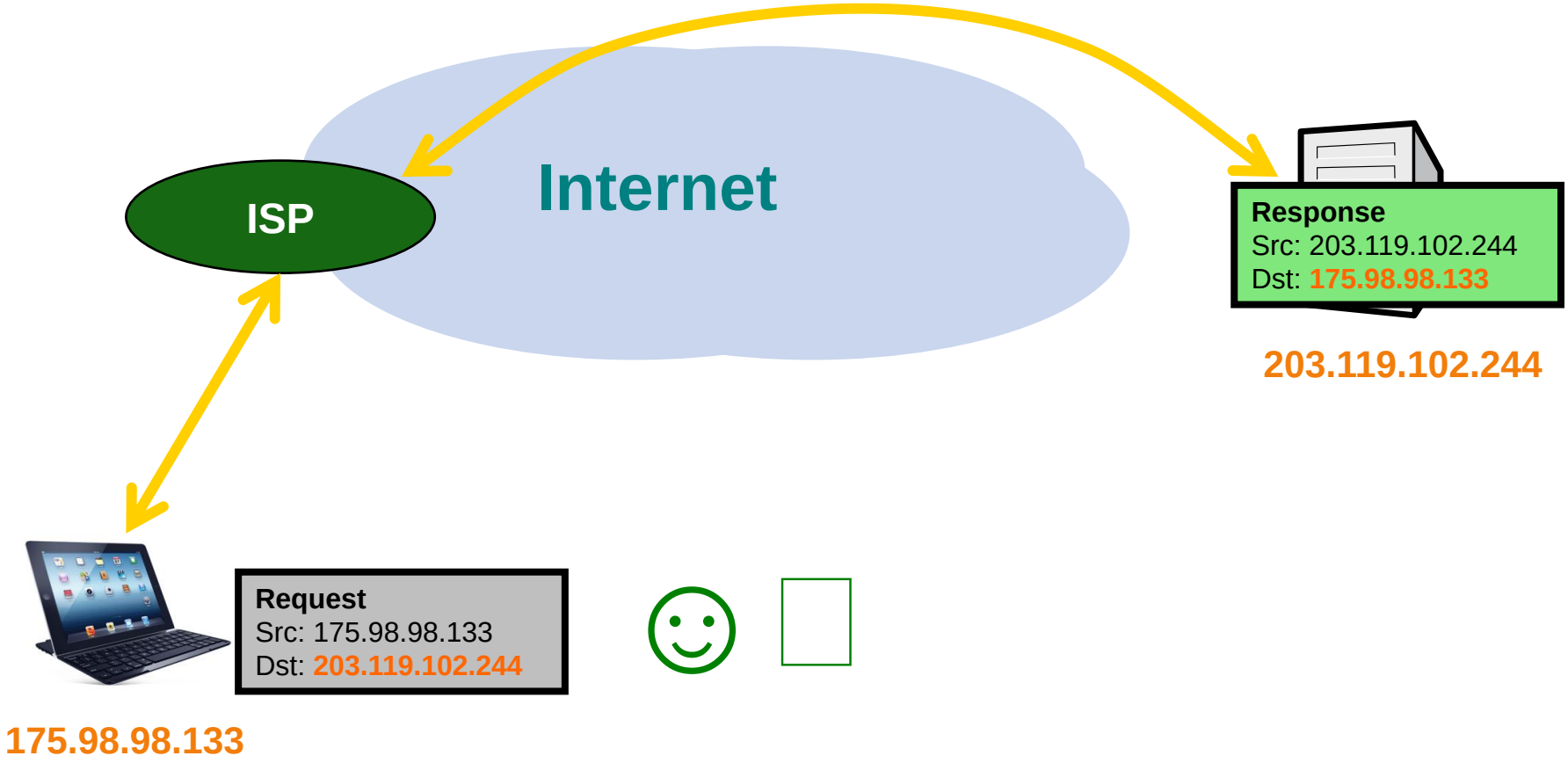
Misusing IP Addresses…



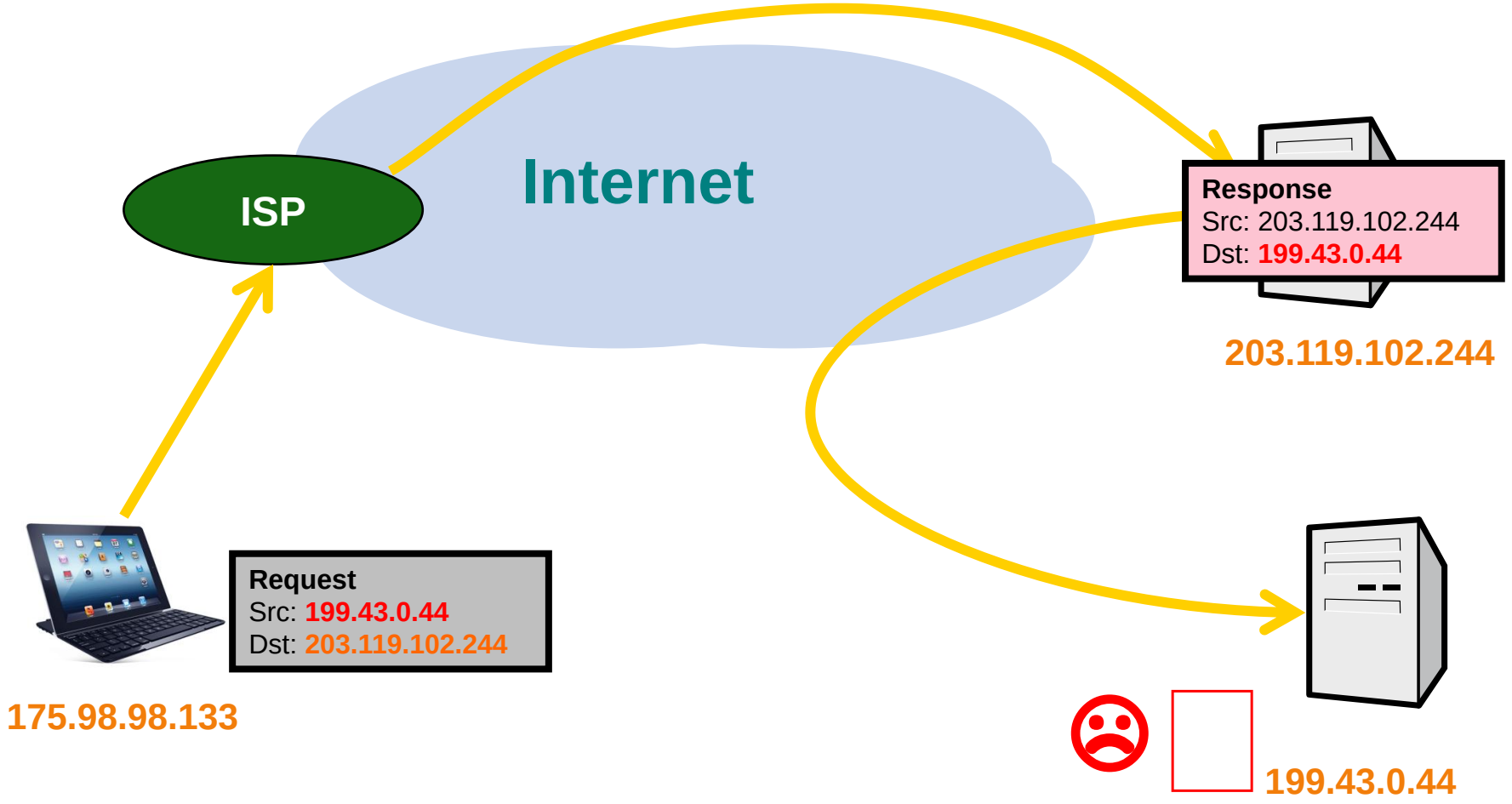
Misusing IP Addresses…



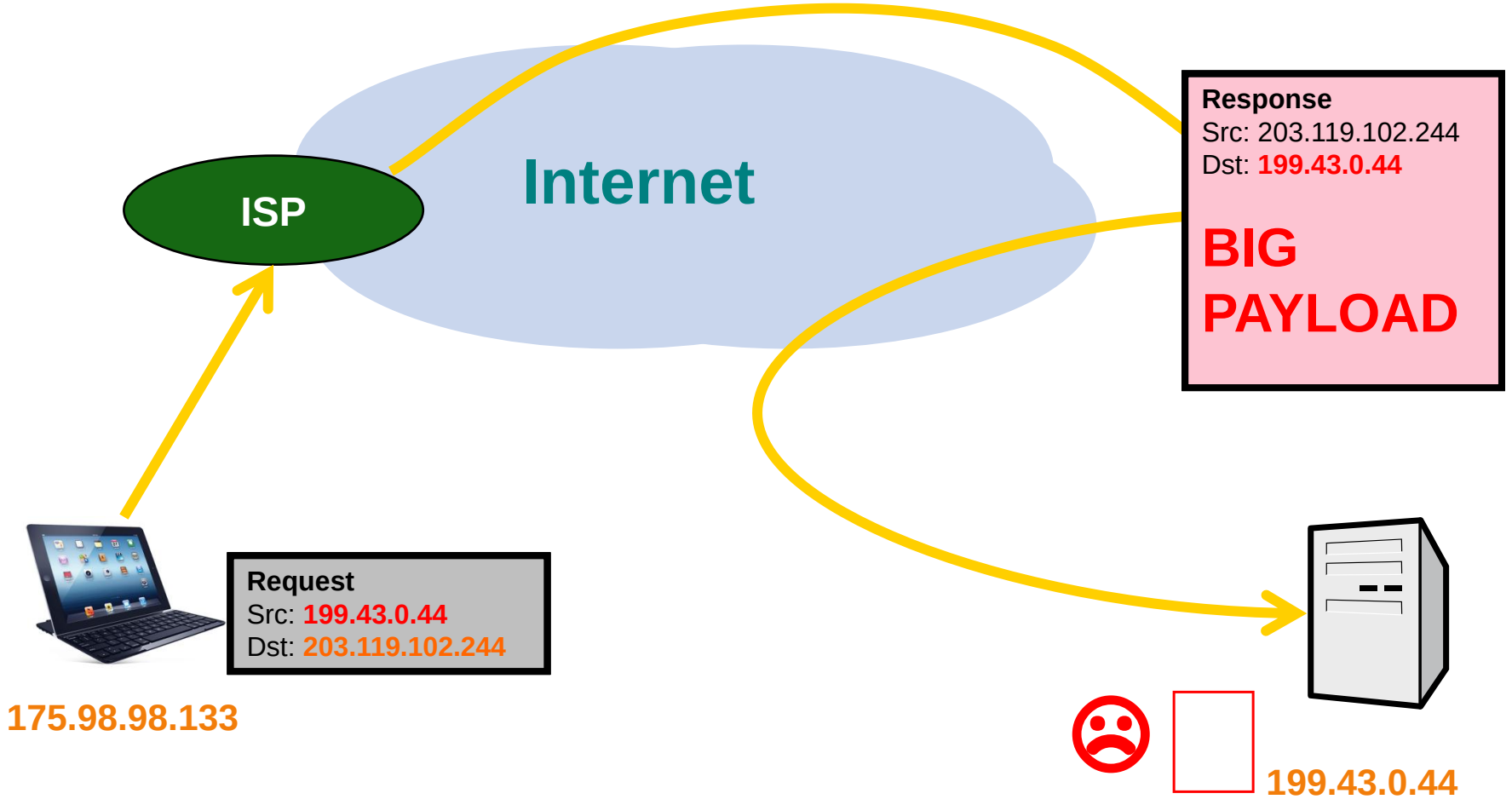
IP address spoofing



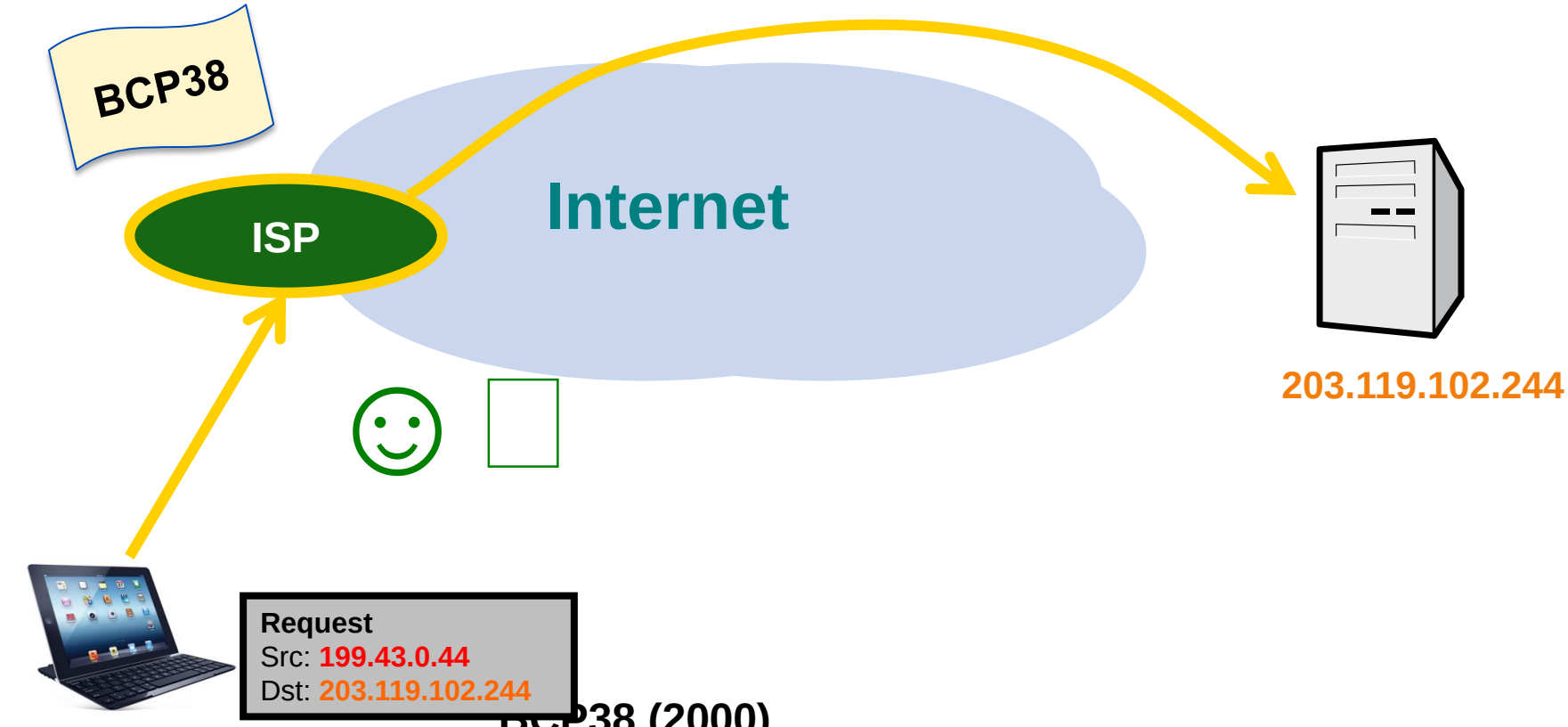
IP address spoofing



DoS attack: Amplification



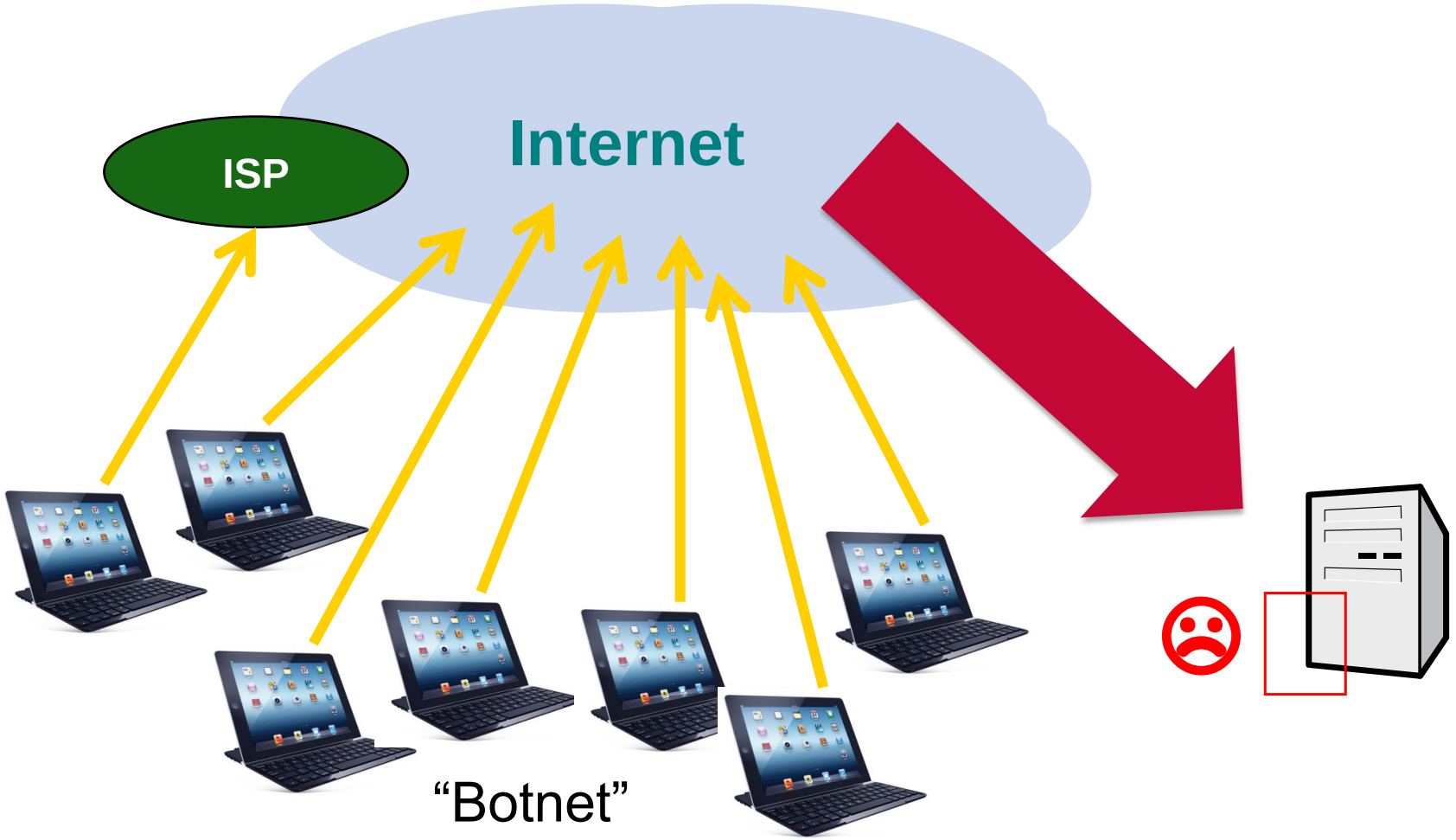
Defeating IP spoofing – BCP38



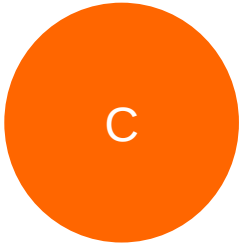
BCP38 (2000)

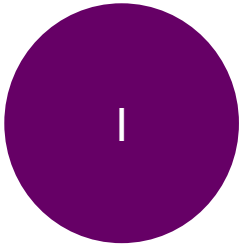
Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

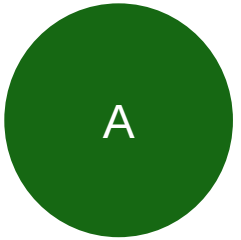
DDoS attack: Distributed DoS



Network Security In A Nutshell

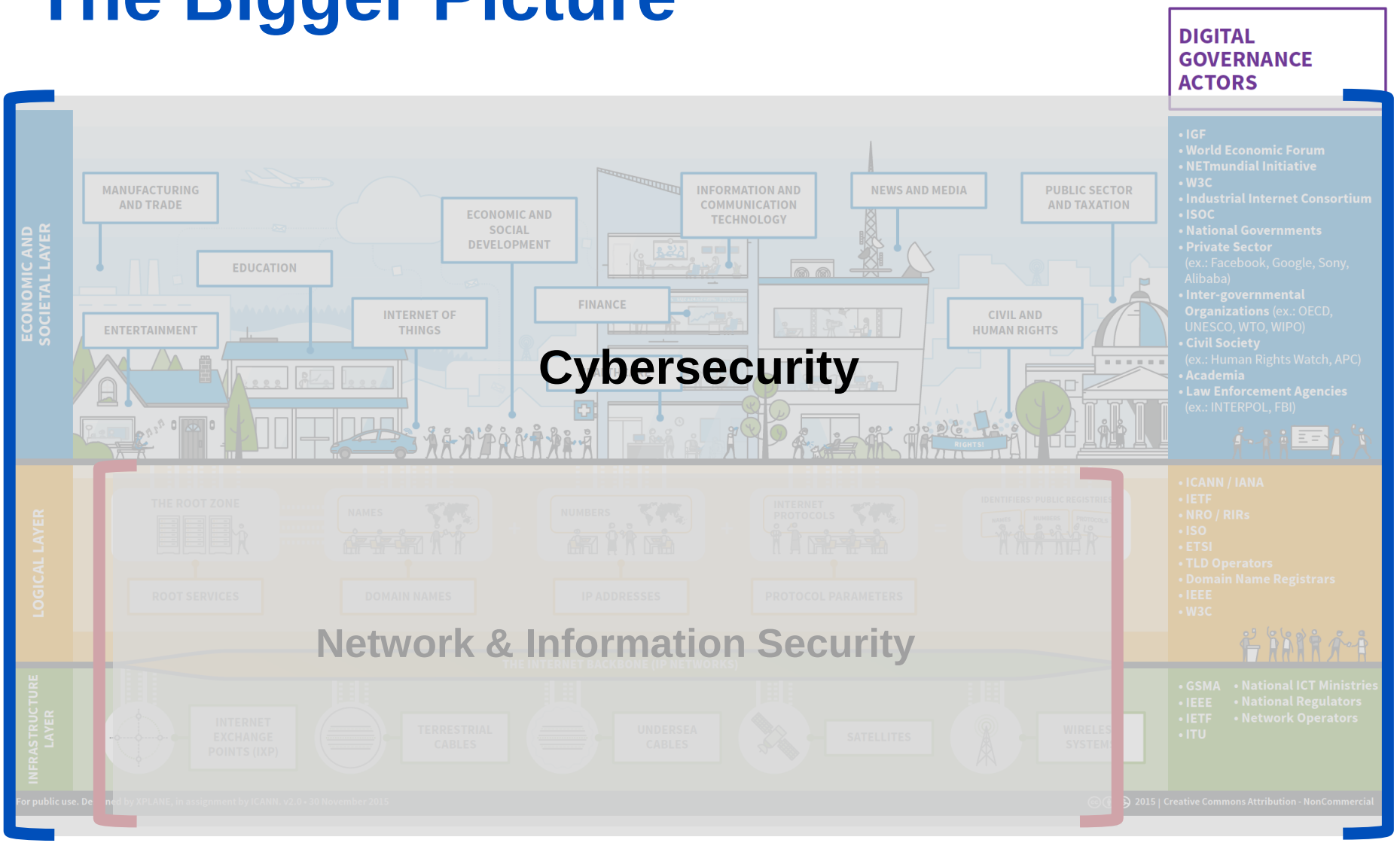




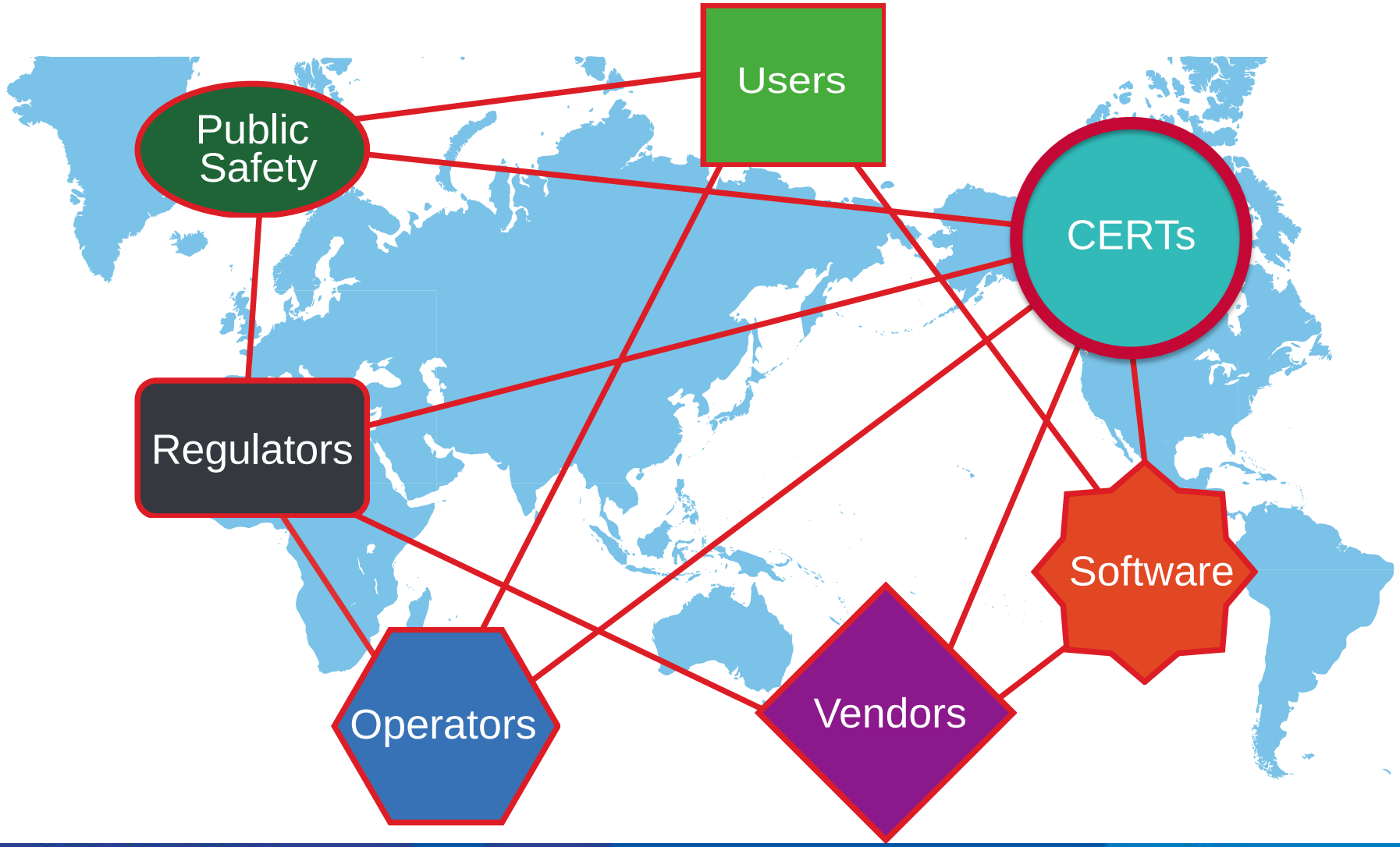


- Ensuring Confidentiality's, Integrity, Availability
- Building a risk management approach
- Implemented through cybersecurity program
- Security as a process
- Technology, people, and process

The Bigger Picture



Internet Security Ecosystem



Asia-Pacific CERTs

incident response

coordination

info sharing

Asia-Pacific CERTs

incident response

Incident Response

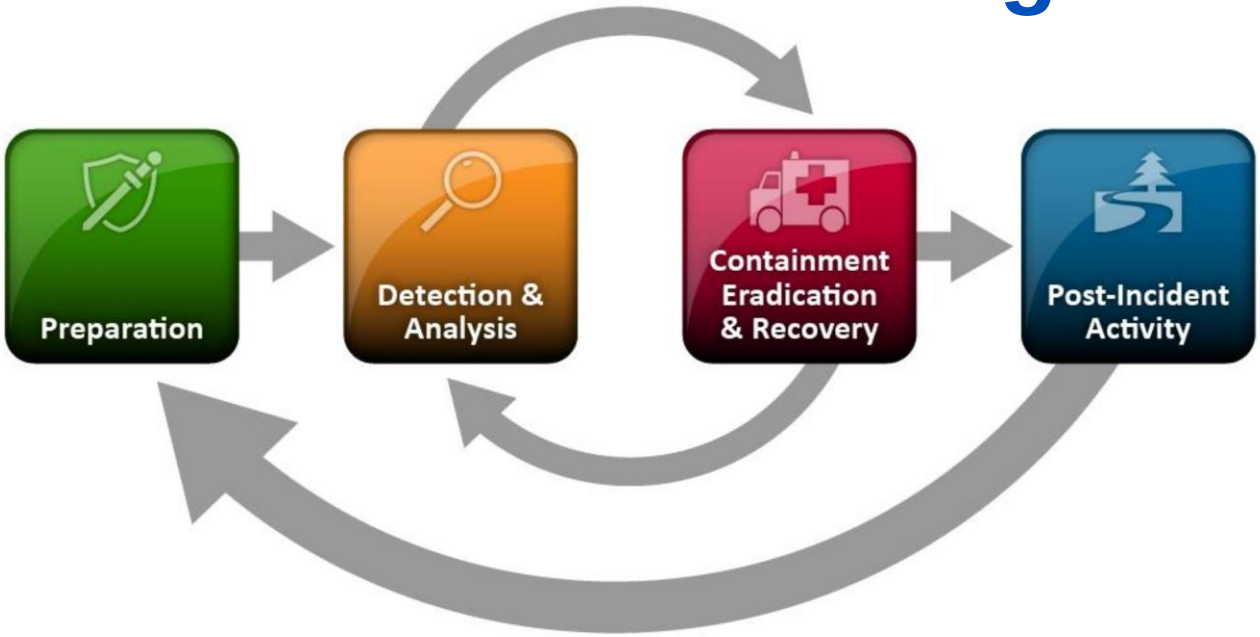
Security Incident

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

- Examples:
  - An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
  - Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  - An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

(Source: NIST SP800-61Incident Handling Guide)

Stages of Incident Handling



1. Preparation
   - Preparing to handle Incidents
   - Preventing Incidents
2. Detection and Analysis
3. Containment, Eradication & Recovery
4. Post Incident Activities

Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Asia-Pacific CERTs

incident response

coordination

Coordination

Source: *NIST Computer Security Incident Handling Guide*

Asia-Pacific CERTs

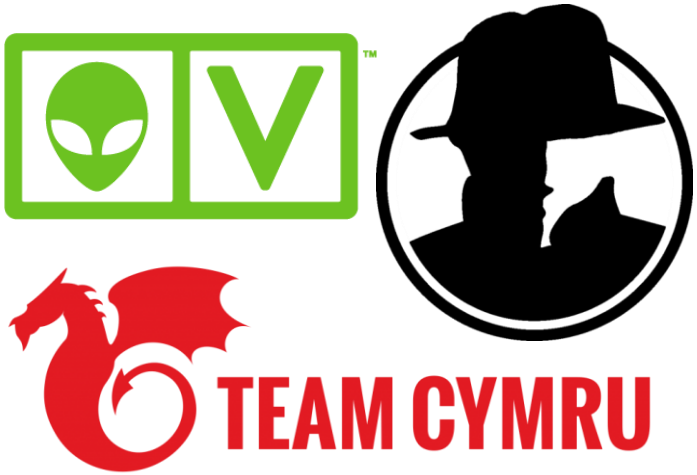
incident response

coordination

info sharing

Information Sharing

- Trusted Group
- Sharing of threat intelligence
- Co-ordinated Response
- Reach out to the community



Why a Team?

- Dedicated resources for Incident Management
  - Dedicated Service(s)
  - Human Resources
  - Specific Polices and SOPs
  - Expertise & Skillsets
- Structured Incident Management / Handling Procedures
- Integration with other activities Internal & External to the organization
  - SOC / IT
  - CERTs / ISACs etc

Building a
- CERT
- CSIRT

APNIC

Defining a CSIRT

…is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency

- Must react to reported security incidents or threat faced by the constituency
- In ways which the specific community agrees to be in its general interest
- Team = Organization that does Incident Response (IR) work!

Defining a CSIRT

…is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency

- **Operational Capacity**
- **Mandate & Terms of Reference**
- **Defined Structure**

Components of a CERT/CSIRT

Constituency

- Who is the Team meant to serve?

- Constituency help defines:
  - What is the purpose & nature of the CSIRT
  - Who is the CSIRT Serving
  - What types of security incidents the CSIRT handles
  - What are the relationship with other CSIRTs

- Constituencies might overlap
  - Co-ordination is key
  - CSIRT of the “Last Resort”

Different Types of CSIRTs

- National CSIRTs
- Coordination Centers
- Analysis Centers
- Enterprise CSIRTs
- Vendor Teams
- Incident Response Providers
- Regional CERTs

Source: US-CERT https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

Policies & SOPs

- Specific for Incident Response & Handling
- Definition of Security Incidents and Related Terms
- Define Scope, Roles & Responsibilities
- Sharing of Information within the organization or with external parties
- What to do in the event of a security incident
  - Specific SOP for dealing with different types of incidents
  - Forms, Templates, Required information
  - How to reach you outside office hours
- Dealing with Crisis
  - Escalation (Internal & External)
  - Dealing with the Media /Press
- Setting Realistic Expectations
  - Dealing with Service Providers

Team Structure

- Team Models
  - Central Incident Response Team
  - Distributed Incident Response Team
  - Co-ordination Team
- Functions / Workflow
  - Incident Reporting
    - Report from internal or external
  - Incident Analysis
    - What is happening, Impact, Patterns
  - Incident Response
    - Containment, Eradication & Recovery
    - Post-Incident Activity / Recommendations
- How many people do we need in a team?

Services

- **Incident Handling & Response**
  - Core activity
- Advisory / Notification
  - Issue advisory relevant to constituency
- Education and Awareness
  - Promoting best practices
  - Policies and SOPs
  - Cyber Security Exercises
- Information Sharing
  - i.e. Global / Regional CSIRTs groups, ISACS
- Other Services
  - Reactive
  - Proactive
  - Security Quality Management

Types of Services Example
* Enterprise CSIRT *

Proactive Services	Reactive Services	Security Quality Management Services
• Security Alerts • Security Reporting • Security Diagnosis • Monitoring of Websites	• Vulnerability Handling • Incident Handling • Artifact Handling	• Security Consultation • Security Education • Security Training • Evaluation of Technologies

Source: NTT-CERT
https://conference.apnic.net/data/39/150304_ntt-cert-activity_1425447986.pdf

Tools & Facilities

- Basically two categories of tools
  - Managing Incident Reports
  - Tools for analysis
- Handling & Managing Incidents Reported
  - Able to collect & store incidents reported
  - Track status, produce reports
  - Function of system can be mapped to SOP
  - Encryption tools for secure communication
- Security Incidents Monitoring & Analysis
  - Tools for processing or analyzing logs, binaries, network traffic
  - Forensics Tools
  - Tools for information sharing
  - Labs / Separate resources for analysis / testing
  - Tools in the Public domains (i.e. Passive DNS)
- Office / Work facilities
  - Secure room, Office facilities, etc
- Good Resource: FIRST Membership Site Visit: http://www.first.org/membership/site-visit-V1.0.pdf

Building Relationships

- Internal
  - Early buy-in from leadership and constituency
  - Costing
    - The cost tends to vary based on a lot of factors
      - Size of team
      - Services provided
      - Nature of Organisation
    - Start Small
      - Using open source tools
      - Scale up as capability and need grows
- External
  - Becoming of a part of a trusted community
    - Attending Meetings / Conferences
    - Capacity Development (Training)

Asia-Pacific CERTs

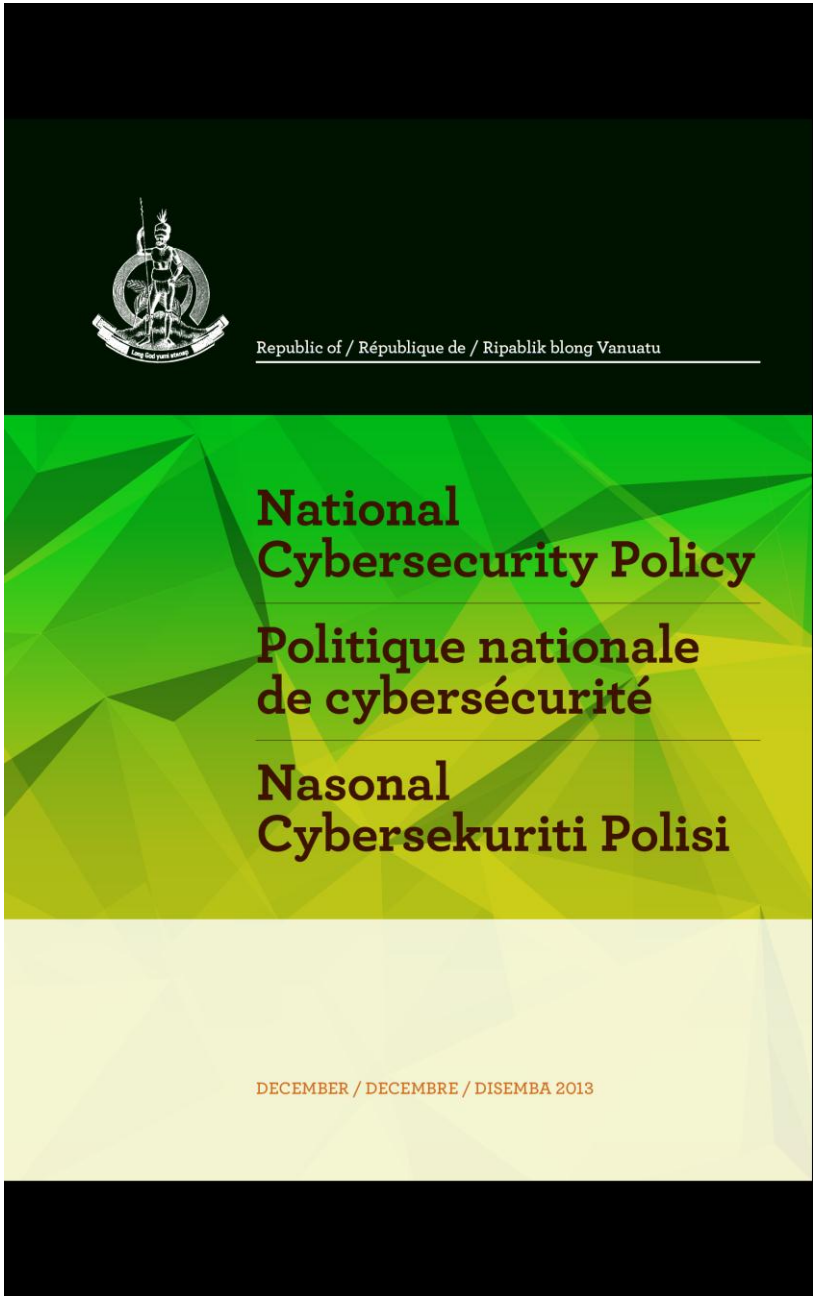
incident response

coordination

info sharing

Road Forward

"Establishment of a National Computer Emergency Response Team (CERT) that is capable of dealing with relevant Cybersecurity threats for citizens, tourists, businesses and government in Vanuatu"



Lets stay engaged!

Upcoming security engagements:

- APCERT Conference | Tokyo, JP
  - 24 to 27 Oct 2016
- NGN Forum | Suva, FJ
  - 1 to 3 Nov 2016
- Technical Assistance | Suva & Nadi, FJ
  - 24 to 26 Nov 2016
- PacNOG 19 | Nadi, FJ
  - 28 Nov to 2 Dec

Adli Wahid
Security Specialist
FIRST Board Member
adli@apnic.net

Klée Aiken
External Relations Manager
klee@apnic.net

APNIC

Tankio tumas!

Questions?