CRYPTREC Symposium 2012

9 March 2012

What's happening out there?

Global Information Security Threats Trends

Dr. Yoichi SHINODA

Professor
Dependable Network Innovation Center
Japan Advanced Institute of Science and Technology

Advisor on Information Security
National Information Security Center (NISC)
Cabinet Secretariat, Government of Japan

> 100G

Largest bandwidth in “bps” observed in 2010 for a single DDoS attack incident. It is 102% increase compared to 2009 record, and 1000% increase compared to 2008 record.

Source: Arbor Networks “Network Infrastructure Report Vol. VI”, Feb. 2011, http://www.arbornetworks.com/report

+ 200%

Increase in number of matching patterns for malwares targeted for Android smart phones in one month. (243 for Sep. to 533 for Oct. 2011)

Source: Trend Micro “ Virus Buster Mobile for Android”

1 / 300

In Oct. 2011, one out of every 300 e-mails contained malware attachments. 47% of these malwares contained links to malicious web sites.

Source: Symantec white paper “The Changing face of Malware Threats”, Nov. 2011.

98%

Customer web sites of a diagnostic service, with some degree of vulnerability; “low” level detected for 7%, “medium” detected for 23%, “High” detected for 37%, multiple “high” detected for 33%.

Source: Secure Sky Technologies actual service record for Jan. 2007 – Dec. 2008

The Outline

1. Changes In The Long Term Threat Trend
2. Trends 2010-2011
3. Trends 2011-2012
4. Change of Game
5. Concluding Remarks

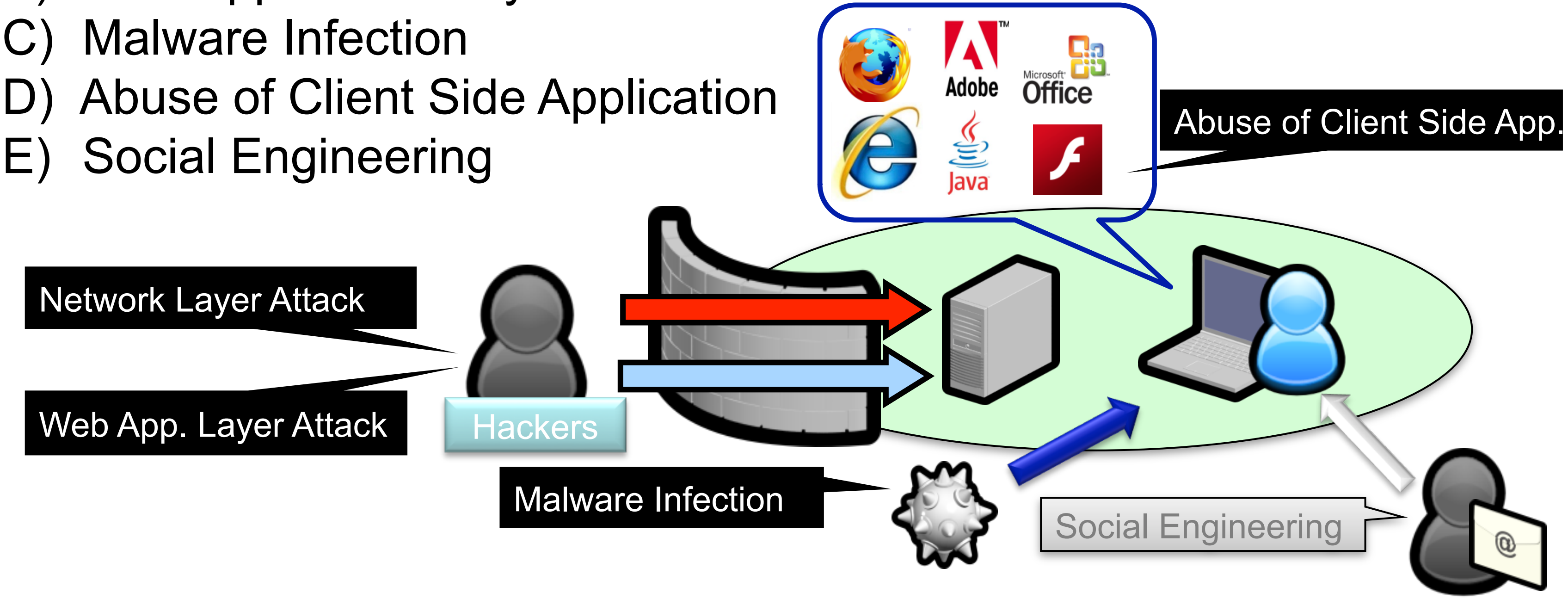
π

1. Changes in The Long Term Trend

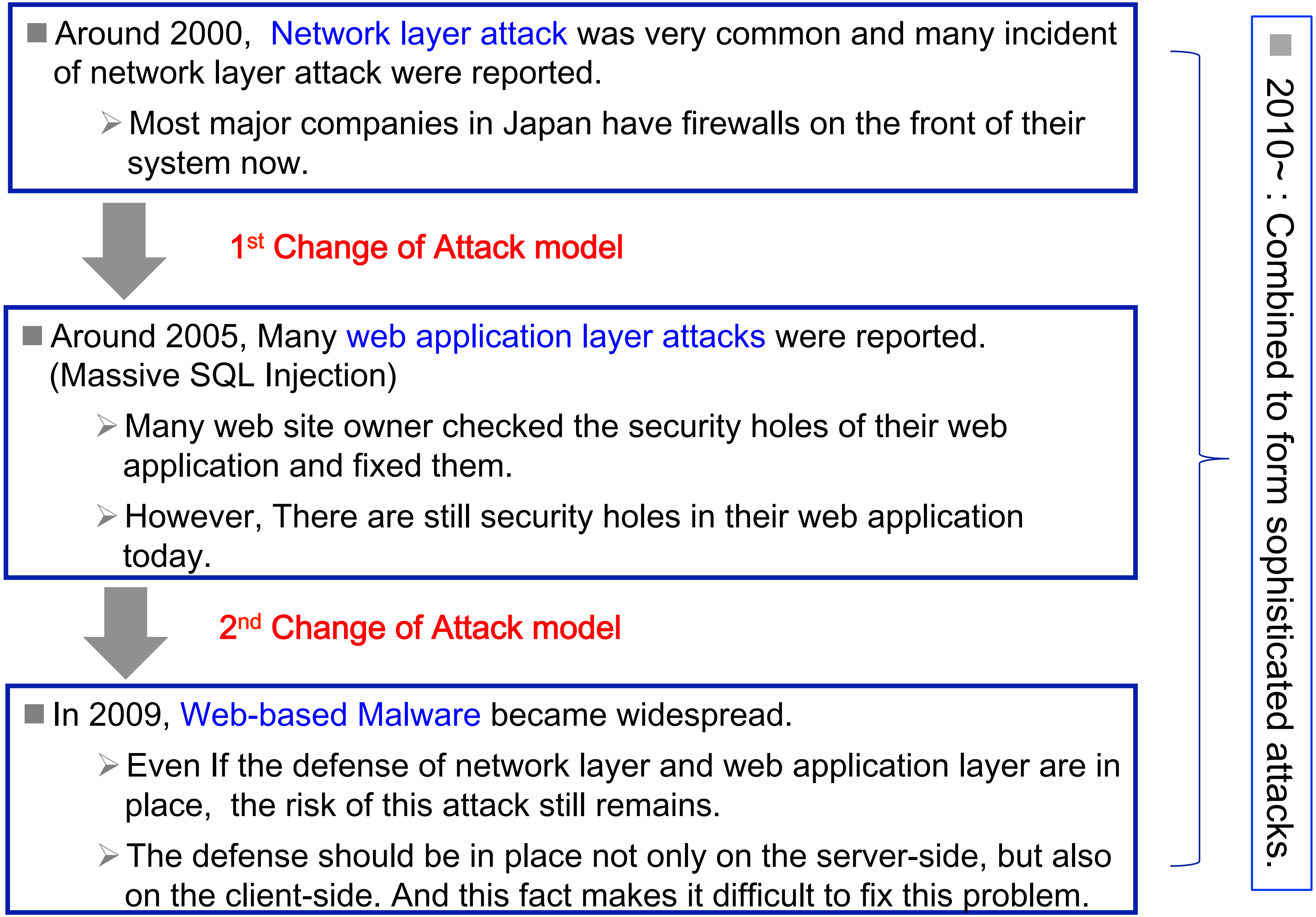
A Taxonomy of Information Security Threat

Threats from the attack vector perspective

A) Network Layer Attack
B) Web Application Layer Attack
C) Malware Infection
D) Abuse of Client Side Application
E) Social Engineering



Changes In The Attack Model



- Around 2000, Network layer attack was very common and many incident of network layer attack were reported.
  - Most major companies in Japan have firewalls on the front of their system now.

1st Change of Attack model

- Around 2005, Many web application layer attacks were reported. (Massive SQL Injection)
  - Many web site owner checked the security holes of their web application and fixed them.
  - However, There are still security holes in their web application today.

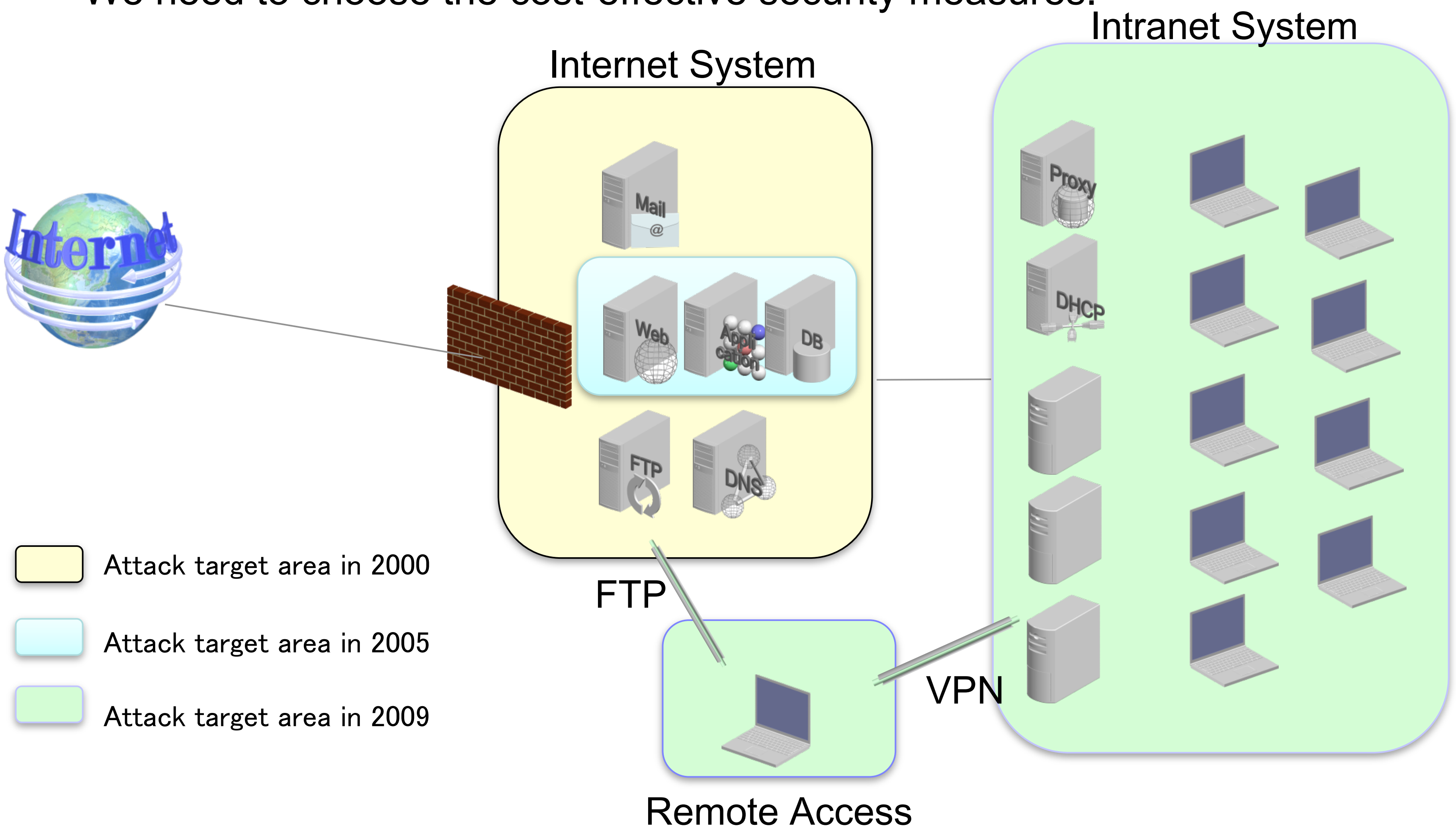
2nd Change of Attack model

- In 2009, Web-based Malware became widespread.
  - Even If the defense of network layer and web application layer are in place, the risk of this attack still remains.
  - The defense should be in place not only on the server-side, but also on the client-side. And this fact makes it difficult to fix this problem.

- 2010~ : Combined to form sophisticated attacks.

Changes In The Target Area

In 2009, The attack target area is getting larger in spite of the fact that other area is not covered adequately.
We need to choose the cost-effective security measures.



Intranet System

Internet System

FTP

VPN

Remote Access

🟨 Attack target area in 2000

🟦 Attack target area in 2005

🟩 Attack target area in 2009

2. Trends 2010-2011

Drive-by Download & The Gumblar

- Drive-by download is an act of unauthorized downloading of (often malicious) piece of software.
- The Gumblar (late 2009 ~ 2010) combined several exploits:
  - Content management system for a web server is infected by drive-by downloading.
  - Passwords for the web server is stolen.
  - Links to drive-by download site are injected into the web server.
  - End users visit the infected (injected) site, forced to drive-by download.
  - If the user's system is another CMS, then the Cycle repeats.
- The Gumblar introduced a new class of attack model: Web-based malware.
  - Measures for the web-based malware is very difficult. It requires integrated approach on both PCs and servers.

Stuxnet and Its Impact

- Stuxnet is an windows worm that spreads through mountable external storage devices (USB memory, smart phones, digital picture frames, voice recorders) and sometimes through network shared storage.
- Looks for a specific system (Siemens FA systems).
- Utilizes 5 exploits, of 2 are zero-day.
- Signed by stolen certificate (looks like a legitimate piece of software).
- First appearance is believed to be around Jan. 2009, but it was not found until June 2010.
- The impact of the Stuxnet is very serious:
  - It penetrate and spread into what so called “closed, physically isolated, dedicated systems” (has some level of commonality with Conficker).
  - It is intended to attack FA systems (including critical infrastructure control systems).

Route Hi-Jacking / Censorship Leakage

- Route hi-jakcking is caused by (intentional or unintentional) injection of illegitimate route information, causing Internet packet detouring or blackholing.

- Examples of 2010 Incidents
  - Mar. 3 – 24, 2010: Routes to a censored instance of DNS root servers in China were leaked to the Global Internet, responded to queries for censored web sites with bogus addresses. The incident affected large number of Internet users around the world (mostly in Asia-Pacific region).
  - Apr. 8, 2010: AS23724 CHINANET-IDC-BJ-AP IDC, China Telecom. Corp. has accidentally originated (hi-jacked) as many as 37,000 unique prefixes for the duration of 15min.

- Observations
  - Classic route hi-jacking tends to occur more frequently.
  - The DNS root server case above, which may represent a new class of route hi-jacking, need more study.

Good Old DoS (Denial of Service) Attacks

- DoS attacks are very common around the world today; we can observe artifacts from hundreds of DoS incidents everyday.

- Some are executed for economic-crime purposes and some are executed for expressing some kind of propaganda. The latter tends to become larger.

- Recently Observed DoS incidents
  - Late September, 2010
    - Large DDoS and associated more sophisticated attacks were placed against wide range of Japanese Internet Infrastructure.
    - Minimal damage was reported.
    - Mitigation efforts
      - Gov. mitigation coordinated by NISC, in collaboration with ISPs and Security Operators.
      - Major ISPs are equipped with modern DoS mitigation devices, and they are experienced.
  - Early December, 2010 (and Continuing)
    - Cyber-propaganda cross-fire between Wiki-Leaks supporters and oppositions.

3. Trends 2011-2012

“Update 2010” summaries and followups (1)

- Drive-by Download & Gumblar
  - Gumblar-like attacks are observed very recently (forged anti-virus softare; an old vector, combined with Server-PC ping-pong infection)
- Stuxnet and Its Impact
  - New malware utilizing Stuxnet modules are now emerging.
  - New initial vector is predicted; vulnerable smart devices as active carriers.

“Update 2010” summaries and followups (2)

- Route Hi-Jacking
  - Large incidents are not reported for 2011; small incidents are daily.
- Good Old DoS
  - Still a very popular and handy tool for expressing an one’s or group’s intention.
  - Mitigation technology is available in a limited manner.
  - New observations
    - Small DoS incidents are observed ***VERY*** frequently.
    - These are sometimes understood as part of a “DoS scanning”.
    - Intentions behind the attacks are unknown, no clear linkage to actual large scale attacks.

2011 Updates (1)

- New classes of advisory party
  - ***Hactivists*** became conspicuous.
    - Frequent activities by hactivists (loose community of hacker activists), e.g., "Anonymous" and "Lulzsec" were observed.
    - The activities were triggered by impulsive events, often put large organizations such as national governments and global enterprises into jeopardy.
  - Existence of ***APT*** (*Advanced Persistent Threat*) became clear.
- Cyber Space now widely (and officially for some counties) recognized as a field of confrontation, in many aspects.
- Malwares targeting smart phones is showing rapid growth.
  - Trend Micro Oct. 2011 report (+200% growth Sep. to Oct.)

Rise of the APTs

Advanced Persistent Threat (APT) usually refers to a group with both the capability and intent to persistently and effectively target a specific entity.

- *Advanced*
  - Operators of APTs have a full spectrum of intelligence-gathering capabilities, including computer intrusion technologies and conventional technologies such as wire-tapping.
  - Often combine multiple targeting methods to produce more sophisticated methods to gain and maintain access to the target.
- *Persistent*
  - Operators give priority to a specific task, rather than the opportunistically seeking gains.
  - Targets are constantly monitored, often by “low-and-slow” approach.
  - Operator’s goal is to maintain long-term access to the target.
- *Threat*
  - APTs are a threat because they have both capability and intent.
  - The operators have a specific objective and are skilled, organized, and often well funded.

2011 Updates (2)

- More and more “previously believed-to-be-secure” things now became (potential) threat vectors:
  - Security tokens:
    - A security token vendor has disclosed that some of the internal information was stolen.
  - Certificate Authorities and certificates:
    - A certificate authority was compromised, and was forced to issue forged certificates, resulting in possible vulnerabilities in multiple major global portal sites.
    - Certificate revocation mechanisms are very poorly implemented in the real world “smaller” devices; smart phones, ubiquitous devices, …

2011 Updates (3)

- E-mails from business partners (or look a likes)
  - E-mails forged to look like they are legitimate, in terms of sender address, subject, attachment names and body text, now may contain fatal attack vectors.
  - In 2012, the NISC conducted a training on targeted e-mail attacks.
    - Subject: Kasumigaseki-resident government employees (60,000)
    - Method: Two mails were sent for each subject, one contained an attachment, another contained a web link.
    - Result:

      Attachment: 10.1% avg. (1.1 - 23.8% depending on the institution) of subject opened the attachment.

      Web link: 3.1% avg. (0.4 – 6.1% ditto) clicked on the link.

2011 updates (4)

- Non-web service targeted DoS attack is predicted.
- New breach in a trust mechanism: a DNS resolver file.
  - Modifies hosts' "resolv.conf" file to redirect ***all*** access to the network at attacker's will.
  - The original attacker was arrested, but the forged DNS server is still run by LE to prevent additional damages to victims.
- Rapid shift to cloud based computing revealed non-readiness of security operations.
  - XaaS layered service model/business makes forensic analysis extremely difficult.
  - Networked computers made damage assessment hard, cloud makes it even harder.

Did Network Attacks Become A History?

- Question: With raise of Web-based attacks, common installation of firewalls, and users shifting to newer operating systems, did network attack become a history?

- Answer: No.
  - New vulnerability in wide range of software and systems are still reported everyday.
  - Network attack is still very active according to network monitors (such as nicter by NICT).
  - Presence of the comprehensive bot networks amplifies effect of newly found vulnerabilities (e.g.: Welch, Conficker, …)
  - Vulnerabilities are utilized for intranet network attacks.

  - Small networking devices are often under-maintained, and like to have multiple vulnerabilities.
- Likewise, Web-Application Layer attacks (SQL injections) are still very common.

Web Applications are inherently vulnerable?

Web applications are inherently vulnerable to attacks:

- *Distributed Nature*
  - Unlike the traditional applications, web applications inherently deals with distributed components and services; even secure components and services become unsecure when they depend on unsecure remote components and services.
  - Web programming facilities are often introduced with functionality (aka “richer user experience”) as the first priority; security considerations are often very weak.
  - The WASC (Web Application Security Consortium) has identified 34 different classes of web application attacks and 15 different classes of weaknesses of web applications that can be attacked.
- *Market Pressure*
  - Most web applications have severe TTM (Time to The Market) schedule.
  - Most web applications are believed to be “lighter” than traditional hard coded applications, thus can be made “cheaper”.
  - Most web applications are required to “be fancy”, not “be secure”.

4. Change of Game

Awareness Rising

Awareness rising plays one of the central role in possible measures.

- Awareness rising in different sectors
  - Government
  - Private industries and enterprises, and supply chains
  - General Public
- Awareness rising has direct and indirect effects
  - Prevent direct damages; large portion of sophisticated attacks are triggered by careless or ignorant operations.
  - Incubate a common sense among people and industries, in investments into security aspects of ICT systems.

From R&D perspective

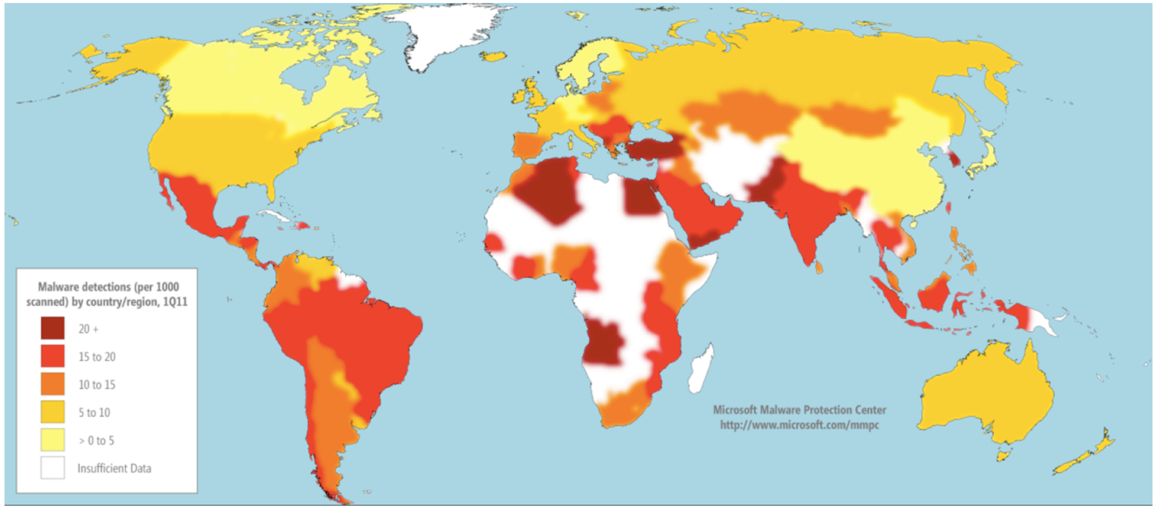
NITRD CSIA IWG "Cybersecurity Game-Change / Research and Development Recommendations" (May 2010)

- Recognition of the current state of the game
  - The cost of attack is asymmetric, and favors the attacker.
  - The cost of simultaneously satisfying all the cyber security requirement of an ideal system is prohibitive.
  - The lack of meaningful metrics and economically sound decision making in security results in a misallocation of resources.
- Proposed way of changing the game
  - Make cyber assets a moving target.
  - Create a trustworthy cyberspace (subspace) model.
  - Create a framework of economic incentives to reward secure practices and discourage bad actors.

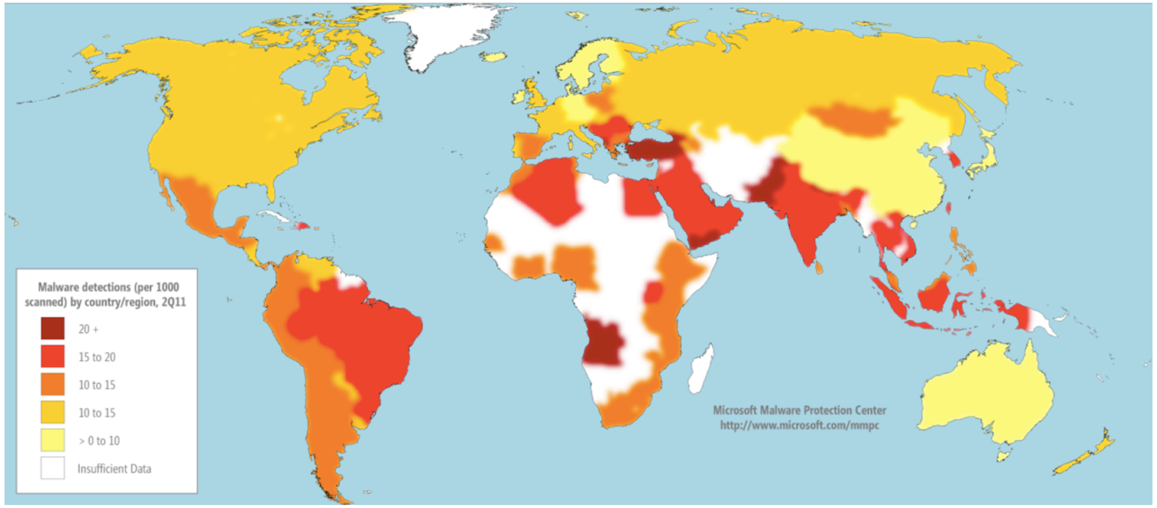
5. Concluding Remarks

Malware Infection Rates by Countries/Regions

1Q2011


Malware detections (per 1000 scanned) by country/region, 1Q11
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

2Q2011


Malware detections (per 1000 scanned) by country/region, 2Q11
20 +
15 to 20
10 to 15
10 to 15
> 0 to 10
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Rates by Microsoft CCM, per 1,000 PCs.

Source: Microsoft Security Intelligence Report Volume 11

Some (personal) notes

- Alice (or Bob) can be adversary now.
- Cryptographically protected channels are making central protection of end-points harder.
  - IDS/IPS can not examine malicious streams.
  - Malware scanners can not examine malicious attachments.
- Poorly maintained “secure” services are often vulnerabilities.