

Cyber security

‘National & International Concerns’

B J Srinath, Sr. Director,
Indian Computer Emergency Response Team (CERT-In)
Ministry of Communications and Information Technology
Government of India

Tel: 011-24363138, Web: <http://www.cert-in.org.in>, E-mail: bj.srinath@nic.in

With the increase in use of information technology, cyber security has assumed a lot of significance, since IT resources can be target, source as well as means of trouble

Cyber Security – Why is it an issue?

Because.....although the threats in cyber space remain by and large the same as in the physical world (ex. fraud, theft and terrorism), they are different due to **3 important developments**

- automation has made attacks more profitable
- action at a distance is now possible
- attack technique propagation is now more rapid and easier

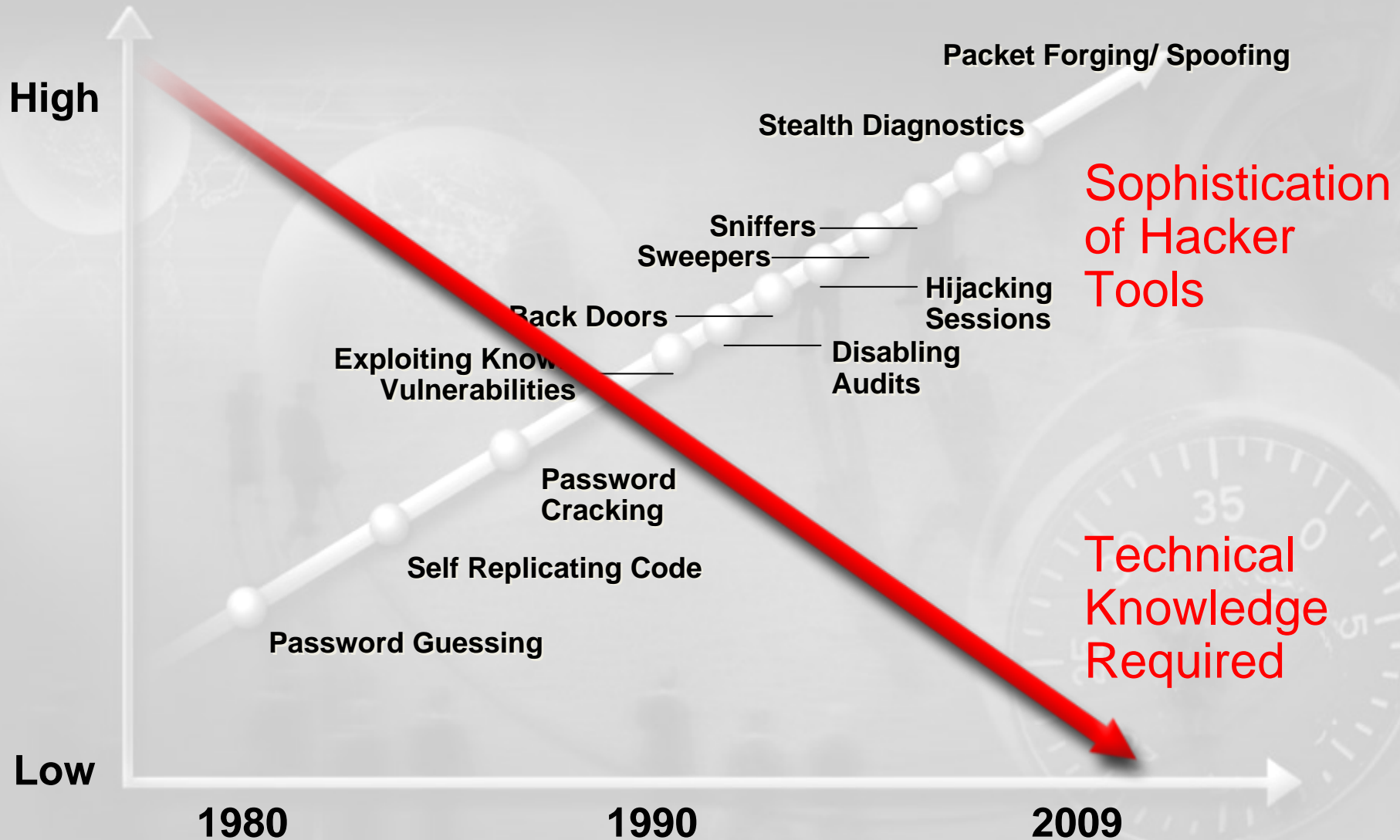
Cyber Security – Why is it an issue?

In addition to the 3 important developments, there are **3 more trends** that make an enterprise transparent and vulnerable

- Internet enabled connectivity
- Wireless networking
- Mobile computing

“Good recipe for trouble – E-Commerce+M-Commerce +
Critical sector plus well known brand-name”

Today's cause for concern



Cyber Security Trends

Recent studies reveal **three** major findings:

- **Growing threat to national security** - web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organized operations aimed at not only financial, but also political or technical gain
- **Increasing threat to online services** – affecting individuals and industry because of growth of sophistication of attack techniques
- **Emergence of a sophisticated market for software flaws** – that can be used to carry out espionage and attacks on Govt. and Critical information infrastructure. Findings indicate a blurred line between legal and illegal sales of software vulnerabilities

Mischievous activities in cyber space have expanded from novice geeks to organized criminal gangs that are going Hi-tech

Stuxnet – The new generation threat

- **Stuxnet** is one of the most complex threats analyzed so far
- It is a **large, complex piece of malware** with many different components and functionalities.
- It was primarily written to **target industrial control systems** or set of similar systems. Its final goal is to **reprogram industrial control systems** (ICS) by modifying code on programmable logic controllers (PLCs) to make them **work in a manner the attacker intended** and to hide those changes from the operator of the equipment.
- It is the first to **exploit** 4 zero-day vulnerabilities, **compromise** two digital certificates, and **inject** code into industrial control systems and **hide** the code from the operator.
- Stuxnet is of such great complexity—**requiring significant resources** to develop—that few attackers will be capable of producing a similar threat, unless **backed by sources with clear ulterior motives**.

It is true that currently ICT resources are being used only as a **support for malicious activities** in the cyber space (such as recruitment, money laundering, information propaganda etc), the recent attacks on Estonia and Georgia and increasing online criminal activities are indeed a pointer towards the potential danger of abuse of ICTs for cyber terrorism and cyber warfare

Security concerns at national level

Considering the **trans-national character of ICT and cyber space**, every sovereign nation would be concerned about

- **Cyber attacks against its ICT infrastructure**, especially critical systems by sources (threat actors, hostile entities or even nation states) inimical to its interest for wrongful purposes and to push their agenda.
- The **technical and legal inability** to clearly identify the perpetrators and sources of attacks entirely on its own, providing freedom to the perpetrators to carry out their acts without fear of detection and counter action.
- **Absence of international mechanism** to facilitate sharing of information for determined actions against the perpetrators and sources of attacks.
- **Lack of adequate trust and confidence** in the commercially available IT products for deployment in critical sectors, owing to assurance-deficit in relation to software bugs, malicious codes, back doors etc.
- **Use of technology** in a way that seeks to influence, interfere and potentially undermine nation state's ability to safeguard its interests as even local laws may prove inadequate (Ex. Encryption).

Security concerns at global level

There are **three specific concerns** that can put the issue of information security beyond the domain of a nation state in the context of international security

- **Deliberate and anonymous use of ICT to target critical infrastructure** of a nation state with a view to causing damage or destabilizing the economy *(Here we are of the opinion that the focus of **non-state actors** would be primarily economic fraud and financial gains, which can be dealt with as cyber crime, whereas the focus of **state-sponsored actors** would be clearly aimed at causing unacceptable damage to the economy and/or creating panic in the society. Hence, we see a clear link between focused attacks on ICT infrastructure and state-sponsored actors)*
- **Unhindered growth of 'network of infected computers' (botnets) across the world**, owing to increased use of ICT and broad band penetration coupled with lack of adequate protective measures at the user end and of course, the ingenuity of those behind the spread of botnets in devising newer methods and effectively using the developments in ICT for their own end *(In our opinion, this threat is the one that makes the threat of attacks on ICT infrastructure more real and more possible, since the **underground economy** facilitates the use of botnets for large and coordinated attacks with a very little possibility of detection, positive identification and counter action. In fact, the rapid growth of botnets can potentially complicate our efforts to put up an effective defense as well as neutralize the sources of attacks)*
- **Risk of misperception**, as nation states contemplate deployment ICTs as instruments of warfare and intelligence, and for political purposes. *(Uncertainty regarding **positive attack attribution** and the absence of common understandings regarding **acceptable State behaviour** may create the risk of instability and misperception)*

Strengthening security at the global level

- India recognises that in the current climate of ICT developments, it is quite possible that **ICT may be used in contravention to the spirit of co-existence and international peace and security**. It is also recognised that since these type of acts can effectively leave a sovereign nation in a state of helplessness, the need for **action by the international community** gains currency.
- Cyber security measures taken by a nation state to protect its ICT infrastructure, coupled with a culture of cyber security, might be capable of providing some level of assurance and confidence, but **will definitely prove inadequate** to deal with the potential threat of deliberate and hostile use of ICT to influence, attack or undermine the ability of a nation state.

Strengthening security at the global level

As a consequence, **India emphasizes** that every country has a:

- **Responsibility to protect** its information and information infrastructure in tune with its national interest and priorities; and
- **Legitimate right to determine** suitable measures to counter the threats of deliberate and hostile use of ICT against its interest.

Under these circumstances, India feels that there is an **imperative need for a set of measures by international community** to:-

- Effectively **address the security concerns** of nation states; and
- **Assist and enable the nation states** in dealing with issue of hostile use of ICT and invoke adequate measures to defend their national interests.

Security at the global level – Our expectations

- Every nation would do what is necessary to **protect its ICT infrastructure and prevent its abuse** and
- International community would do what is necessary to **create a world security eco system** in which the prospect of ICT abuse is reduced to minimum, through a set of cooperative and collaborative actions and in the event a cyber crisis manifests that threatens international peace and security, there would be a coordinated response, in a visible and demonstrable manner, to contain and mitigate the crisis, irrespective of the location of crisis.

Cyber Security - Final Message



“Failure is not when we fall down, but when we fail to get up”

“We want you Safe”

Thank you

