Cyber Security Policy

- Honesty & Truth are Best Policies….

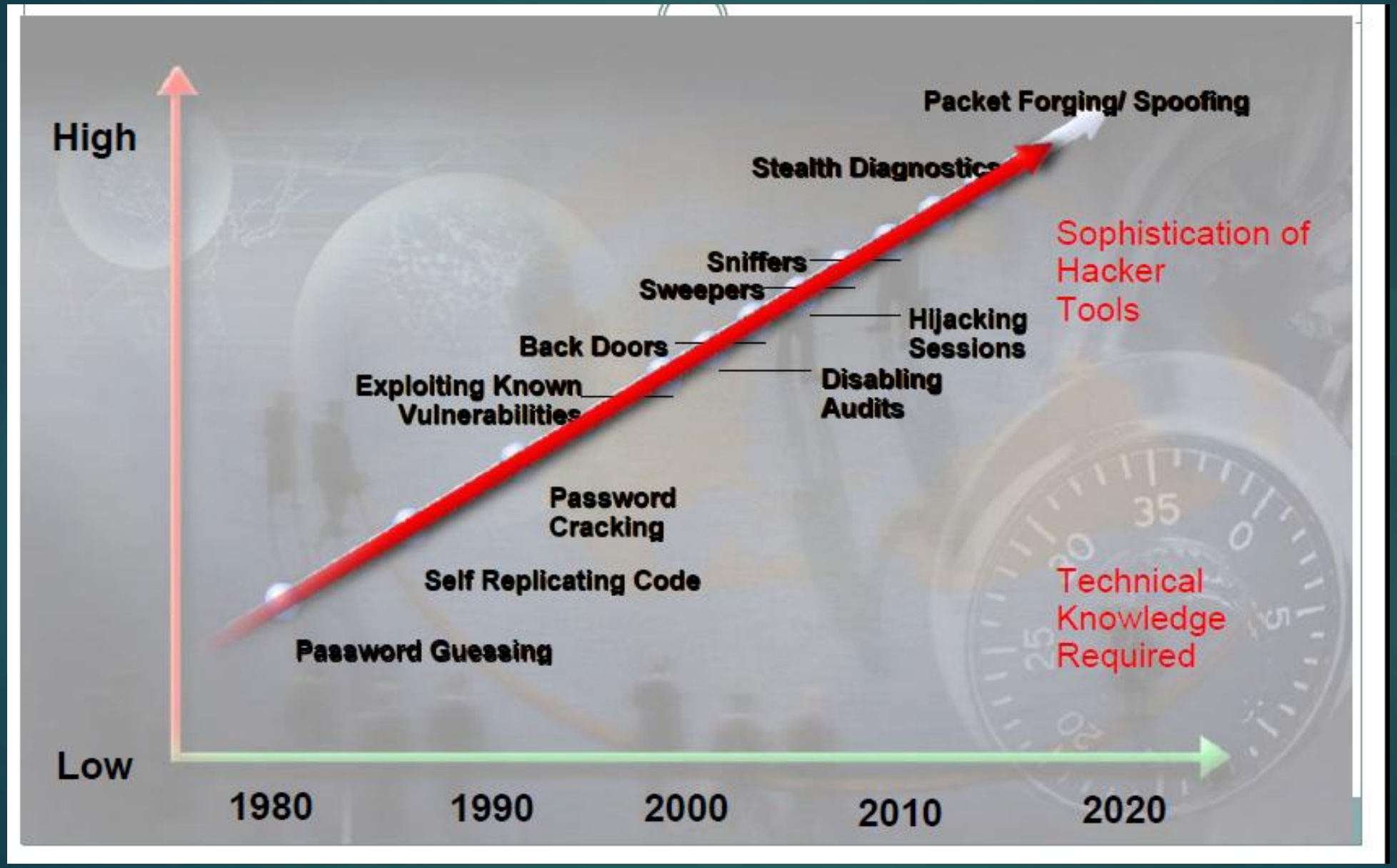
Presented by

Dr. M. Prasad, M.Tech, Ph.D, MISTE, MCSI, MIAENG,,
Professor & Head,
CSE Department,
B V C I T S, Amalapuram

The only system which is truly secure is one which is **switched off** and **unplugged**, **locked** in a titanium safe, **buried** in a concrete bunker, and is surrounded by **nerve gas** and very highly **paid armed guards**. Even then, I wouldn't stake my life on it.

- By Professor Gene Spafford

Why cyber security has become essential now?


High
Low
1980
1990
2000
2010
2020
Packet Forging/ Spoofing
Stealth Diagnostics
Sniffers
Sweepers
Hijacking Sessions
Back Doors
Disabling Audits
Exploiting Known Vulnerabilities
Password Cracking
Self Replicating Code
Password Guessing
Sophistication of Hacker Tools
Technical Knowledge Required

- Mischievous activities in cyber space have expanded from novice to Hi-tech
- Growing threat to national security
- Increasing threat to online services
- Emergence of a sophisticated market for software flaws
- Illegal sales of software vulnerabilities
- Internet has become an weapon for political, military and economic espionage
- Most Govt. agencies and companies around the world use common computing technologies & systems
- Traditional protective measures are not enough to protect against attacks
- National networks with less sophistication in monitoring and defense capabilities
- Exponential growth in social networking sites, social engineering

Why Security policy is required?

- To **Prevent cyber attacks** against the country's critical information infrastructures
- To **Reduce national vulnerability** to cyber attacks
- To **Minimize damage and recovery** time from cyber attacks
- For **creation of a technical-professional body** that certifies the security of a network to ensure the overall health of government systems.

Who is responsible for ensuring virtual space free of cyber threat?

- Government
- Private sector
- Users
- Academicians

Action needed to be taken at different levels

At country level:

- **Policy directives** on data security and privacy protection - Compliance, liabilities and enforcement

  (Ex. Information Technology Act 2000)

- **Standards and guidelines** for compliance

  (Ex: ISO 27001, ISO 20001 & CERT-In guidelines)

- **Conformity assessment infrastructure** enabling and endorsement actions

  (Ex: Security product – ISO 15408, security process – ISO 27001 and security manpower – CISA, CISSP, ISMS-LA, DISA etc.)

- **Security incident** - early warning and response

  (Ex: National Cyber Alert System and Crisis Management)

At country level – Cont.

- **Information sharing and cooperation**

  (Ex: MoUs with vendors and overseas, CERTs and security forums).
- **Pro-active actions to deal with and contain malicious activities** on the net by way of net traffic monitoring, routing and gateway controls
- Lawful **interceptions** and **Law enforcement**.
- Nation wide **security awareness campaign**.
- **Security research and development** focusing on tools, technology, products and services.

Actions at Network level

- **Compliance to security best practices** (ex. ISO27001), service quality (ISO 20001) and Service Level Agreements (SLAs) and demonstration.
- **Pro-active actions** to deal with and contain malicious activities, ensuring quality of services and protecting average end users by way of net traffic monitoring, routing and gateway controls
- **Keeping pace with changes** in security technology and processes to remain current (configuration, patch and vulnerability management)

Actions at Network level – Cont.

- **Conform to legal obligations and cooperate with law enforcement** activities including prompt actions on alert/advisories issued by CERT-In.
- Use of **secure product and services** and skilled manpower.
- **Crisis management and emergency response**.

Actions at small user level:

- Maintain a **level of awareness** necessary for self-protection.
- Use **legal software and update** at regular intervals.
- **Beware of security pitfalls** while on the net and adhere to security advisories as necessary.
- Maintain **reasonable and trust-worthy access control** to prevent abuse of computer resources

HOW THIS POLICY CAN CHECK CYBER CRIMES?

- Governments are likely to get aggressive and pursue action
- Governments will start putting pressure on intermediary bodies
- Industry sector codes of practice
- Greater connectivity, more embedded systems
- Compliance regulations will drive upgrades and changes
- Massive data storing

- *National Cyber Security policy will ensure amendments to Indian IT Act and designing security and privacy assurance framework, Crisis Management Plan (CMP) etc.*
- Formulation of *security standards/ guidelines, empanelment of IT security auditors, creating a network & database of points-of-contact.*
- *Training programs on security related topics and CERT-In initiatives.*
- *Conduct cyber security drills and security conformity assessment infrastructure covering products, process and people.*

- Enabling CERT-In as a `Trusted Referral agency'.
- *Specific actions include –*
    - *National cyber security strategy (11th Five Year Plan)*
    - *National Cyber Alert system*
    - *MoUs with vendors*
    - *MoUs with CERTs across the world*
    - *Network of sectoral CERTs in India*
    - *Targeted projects and training programs for best practices in security and incident response.*
- Public Communication & Contact programs to increase cyber security awareness and to communicate Govt. policies on cyber security.

- Security control emphasis depends on the kind of environment
  - Low risk : ***'Awareness'*** – *know your security concerns and follow best practices*
  - Medium risk: ***'Awareness & Action'*** – *Proactive strategies leave you better prepared to handle security threats and incidents*
  - High risk: ***'Awareness, Action and Assurance'*** – *Since security failures could be disastrous and may lead to unaffordable consequences, assurance (basis of trust & confidence) that the security controls work when needed most is essential.*

“Wish you remain Safe from cyber threat”

Dr. M. Prasad,
Professor & Head - CSE,
prasads.maddula@gmail.com
9959234235