

# **Security on the Internet: The Problem, Solutions and Perspectives**

**Alain Patrick AINA**

`aalain@afrinic.net`

# The Problem(1)

**In the rush to benefit from using the Internet, organizations often overlook significant risks.**

The engineering practices and technology used by system providers do not produce systems that are immune to attack

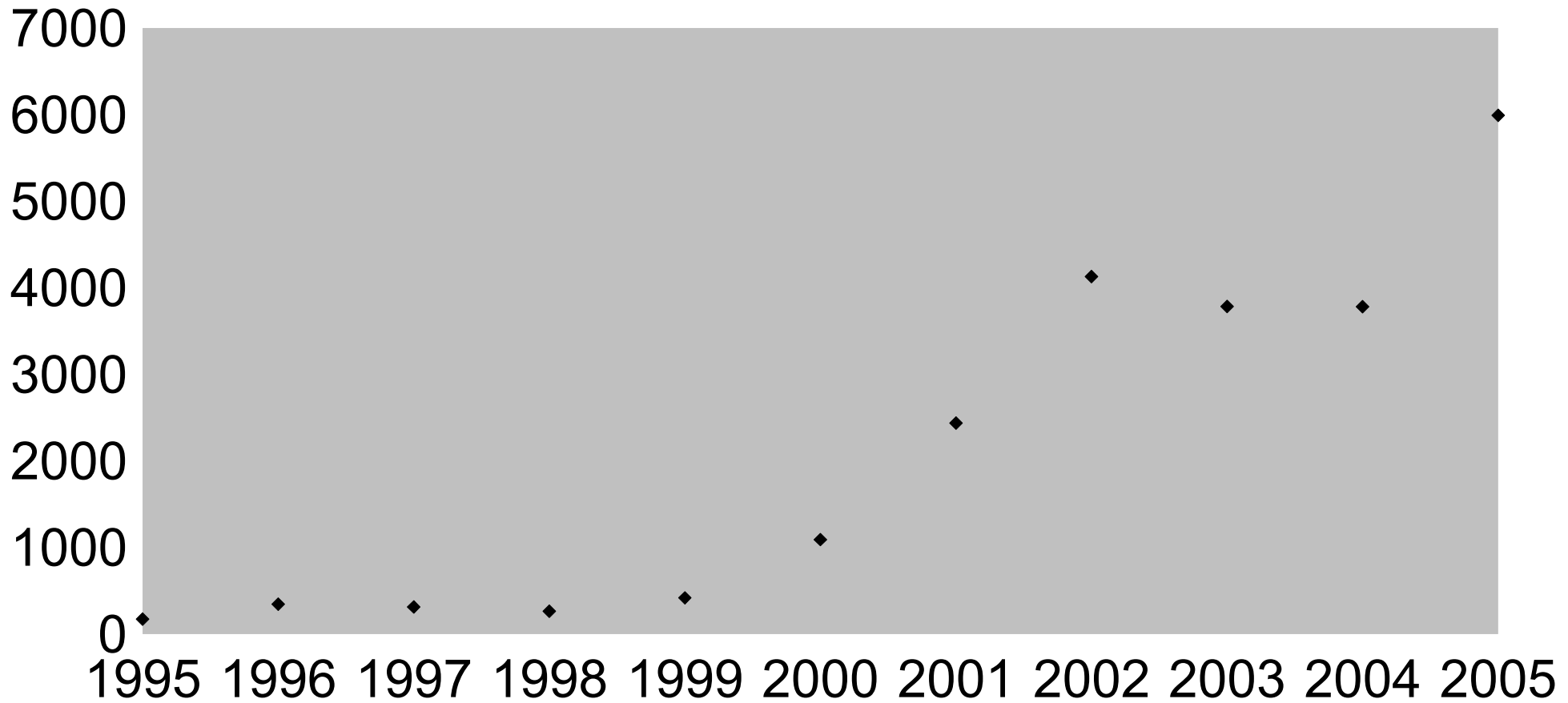
- Network and system operators do not have the people and practices to defend against attacks and minimize damage
- There is continued movement to complex, client-server and heterogeneous configurations with distributed management.

# The Problem(2)

- There is little evidence of security improvements in most products; new vulnerabilities are found routinely.
- Comprehensive security solutions are lacking; current tools address only parts of the problem.
- Users are not educated or do not care.

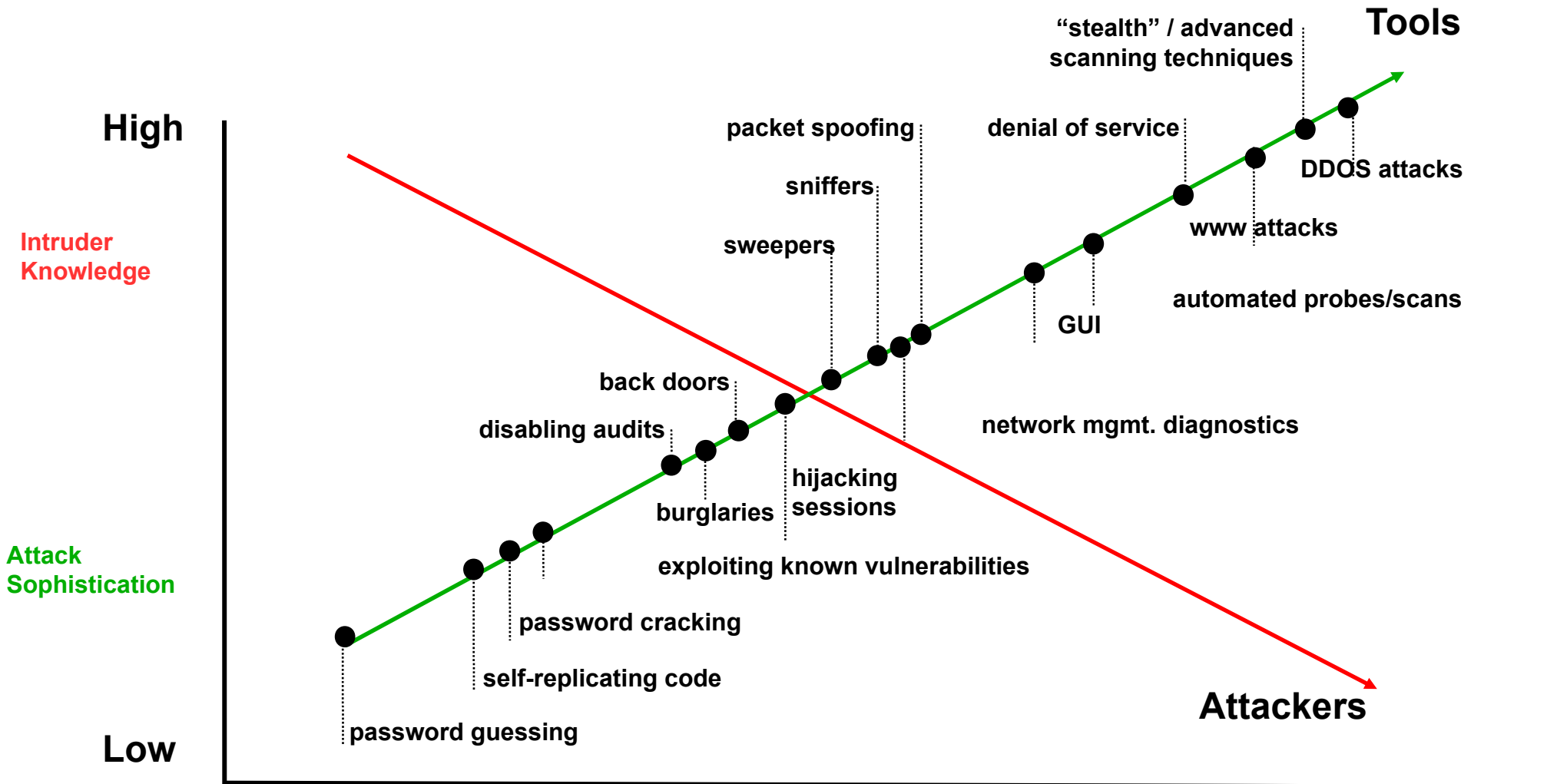
# The Problem(3)

## Vulnerabilities/Year



Source:[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

# The Problem(4)



Attack Sophistication vs. Intruder Technical Knowledge

# The problem (5)

Percentage of important type of incidents : 433 respondents for 2008

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info from mobile devices	10%	9%	9%	8%	9%
from all other sources					4%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data from mobile devices				17%	17%
from all other sources					8%

Source : 2008 CSI/FBI Computer crime and security survey

<http://gocsi.com>

# Solutions

## **BUILDING TRUST ENVIRONMENT FOR E-LIVE**

**What is Africa doing ?**

***The interaction of threat and countermeasure pose distinctive problems for security specialists:***

***The attacker must find but one of the possible multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all.***

# Trainings and capacity building

- AfNOG workshops to increase local engineers security expertises on network and services
- AfTLD training ccTLD operators on ACRP (Attacks and Contingency Response Planning)
  - Arusha, 13-17 April 2009
  - Dakar, 7-11 December 2009
  - <http://www.aftld.org>

# Trainings and capacity building(2)

- AfriNIC/FBI Law Enforcement meeting
  - 01/2010, Mauritius
  - Develop a communication strategy directed to governments and regulators in our Region
  - Focus on IP addressing issues affecting LE
- AF-Cybersec meeting
  - 28/09-02/10 2008, Cote d'Ivoire
- ITU West Africa Workshop on policy and Regulatory Frameworks for Cybersecurity and CIIP
  - 27-29 November 2007, Praia, Cape Verde

# Trainings and capacity building(3)

- Local copies of root servers deployment in our region
  - 9 nodes(2 global nodes) as today
  - Help secure the root server system
  - Allow better access to this critical resource
- Localization of some critical contents
  - Ease OS and tools updates
- End-users education and information campaigns
  - In Kenya
  - Others are following

# Trainings and capacity building(4)

- AfriNIC Anti-Abuse Group(AAAG)
  - Launched last year
  - To focus on E-mail abuses tracking
  - Reserved to AfriNIC members( IP holders)
  - Initiative from the community and supported by AfriNIC

# Securing the DNS

- Many workshops and tutorials on the continent on DNSSEC
- .na(Namibia) is signed

;; ANSWER SECTION:

```
na.          345600      IN      SOA     merlin.net.na. dns-admin.omadhina.net. 2009101516 7200 3600 2419200 21600
na.          345600      IN      RRSIG  SOA 5 1 345600 20091114050401 20091015050401 19392 na.
WdbLOB+h1HTxmizldJbQ3JnpH0lUVvVqx3rklldXAsd/XqgBEWJhK97 QZLV5c95oaLgnr8kR5/L1n71fQv6//8+b/4XySrO022SNPXCf2Stk2V
4Q1EV0gsSBHMB3sa8VjcQFikXrIP22PFOQbmaRPaCkjhL2eQs8LSnl2A 7Q4=
```

- SLDs are being signed and keys published through ISC DLV and other means
- Some of us are validating signed DNS data
- Waiting for the root to be signed.
  - Watching NTIA, Verisign and IANA

# RPKI: Addressing and routing security

- IRs to certify the INRs allocation
  - Certify the “right-to-use”
  - RFC3779 extensions to X509 certificates
- The Resources Public Key Infrastructure (RPKI) to bind together certificates and others signed objects in a verifiable way
- AfriNIC will launch soon its provisioning system
  - To meet the NRO timeline of 01/01/11
  - To issue certificates to LIR and end-users
  - To allow them to issue certs and sign objects