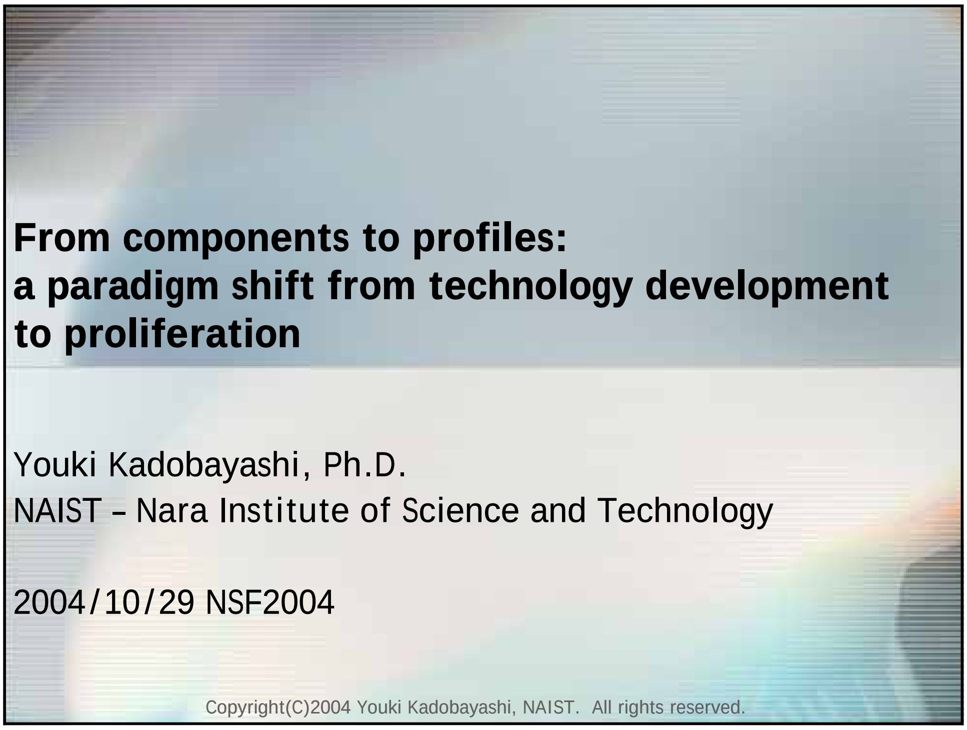
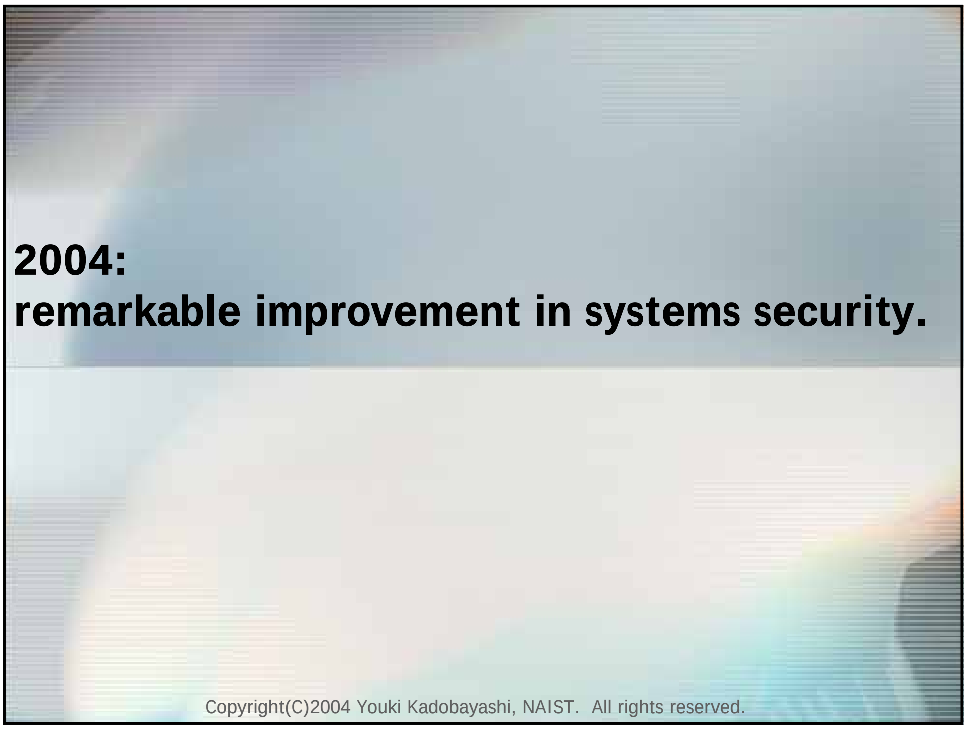


From components to profiles: a paradigm shift from technology development to proliferation

Youki Kadobayashi, Ph.D.
NAIST – Nara Institute of Science and Technology

2004/10/29 NSF2004

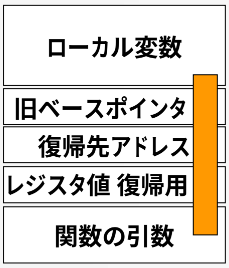


2004: remarkable improvement in systems security.

Before 2004

- Components were fragile, primarily because of:

- Buffer overrun
  - Stack smashing
  - Heap smashing



ローカル変数

旧ベースポインタ

復帰先アドレス

レジスタ値 復帰用

関数の引数

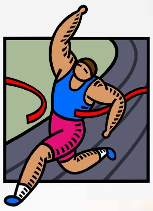
- Resulting in:
  - Nimda, Blaster, Sasser etc.
  - Most vulnerable COTS were targeted

R&D on buffer overrun

- Some precursor work (StackGuard etc.)
- GNU GCC patches
  - Early adoption in FreeBSD, etc.
  - Techie-only spec
- References
  - C. Cowan, C. Pu, et al., “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks”. In *Proceedings in the 7th USENIX Security Symposium*, January 1998.
  - Hiroaki Etoh, “GCC extension for protecting applications from stack-smashing attacks”, available online,
  - http://www.trl.ibm.com/projects/security/ssp/
  - J. Wilander et al., “A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention”. In *Proceedings of NDSS 2003*.

A broader adoption

- GNU GCC patches
  - Adopted by OpenBSD mainstream release
  - Some Linux distributions?
- Microsoft Visual C++ /GS option
  - Adopted in Win2003 Server
    - Defeated Blaster worm
  - Further improved & adopted in Windows XP SP2, Windows Server 2003 SP1



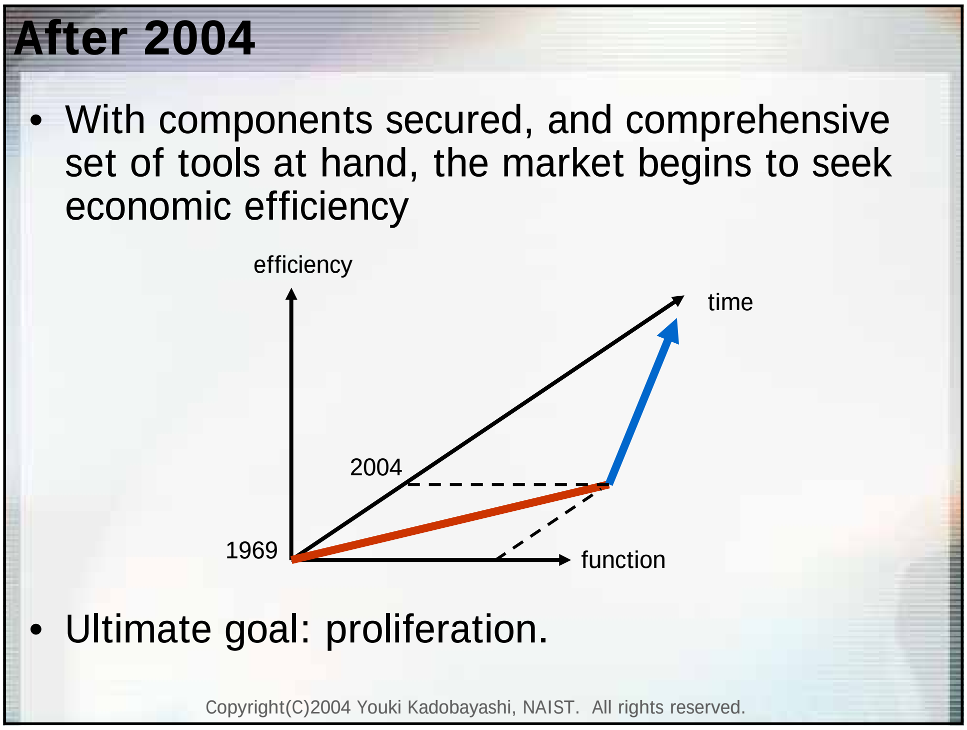
- MacOS X?

For more on /GS (aka software DEP)

- Brandon Bray, “Compiler Security Checks In Depth”, MSDN,
- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dv_vstechart/html/vctchcompilersecuritychecksindepth.asp

- Brandon Bray, “Security Improvements to the Whidbey Compiler”,
- http://blogs.msdn.com/branbray/archive/2003/11/11/51012.aspx

- Microsoft Corporation, “Changes to Functionality in Microsoft Windows XP Service Pack 2”,
- http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx

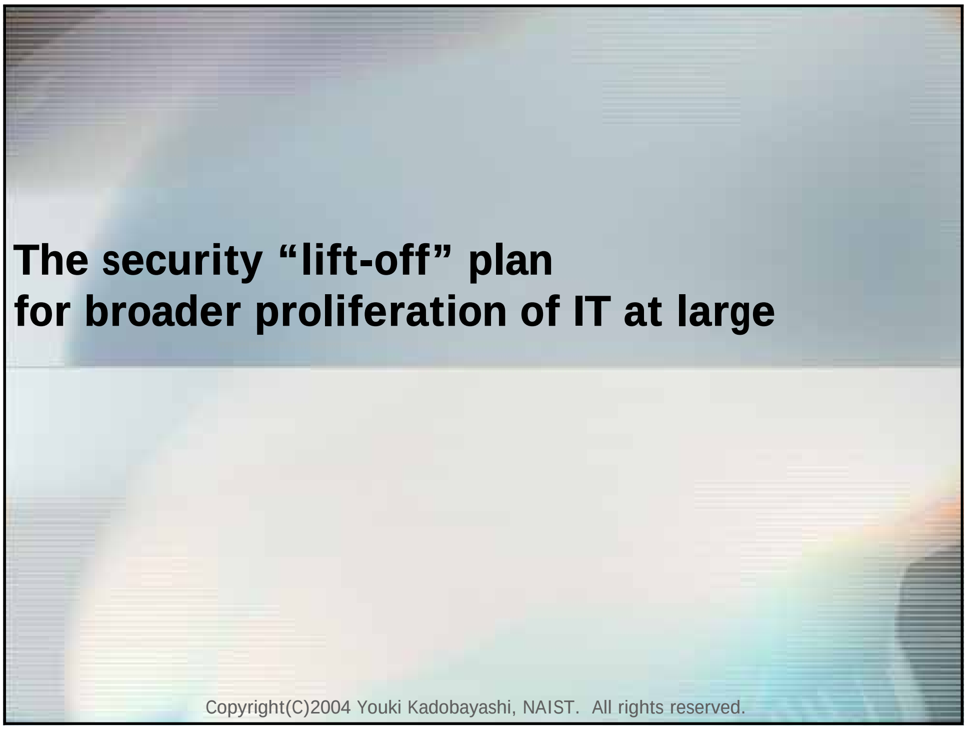


After 2004

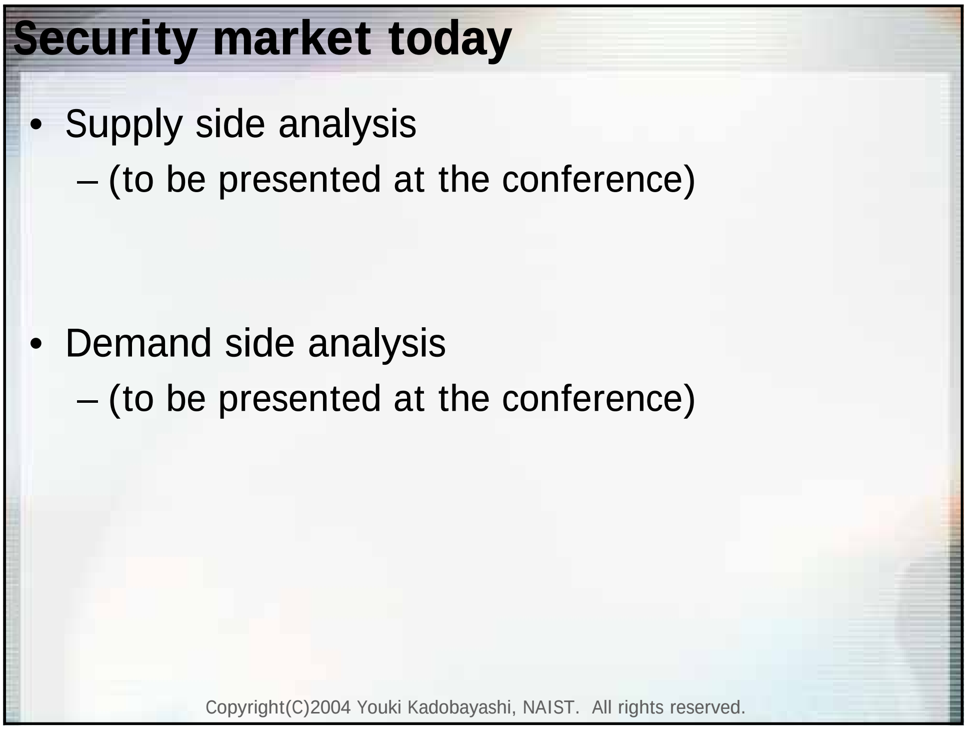
- With components secured, and comprehensive set of tools at hand, the market begins to seek economic efficiency

efficiency
time
2004
1969
function

- Ultimate goal: proliferation.

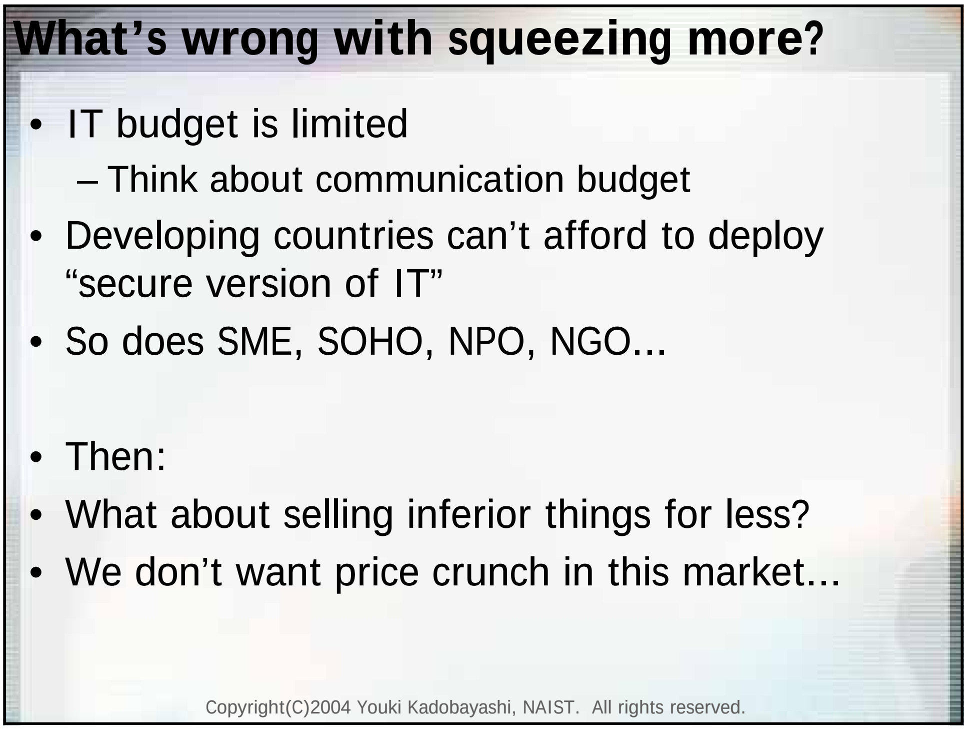


The security “lift-off” plan for broader proliferation of IT at large



Security market today

- Supply side analysis
  - (to be presented at the conference)
- Demand side analysis
  - (to be presented at the conference)

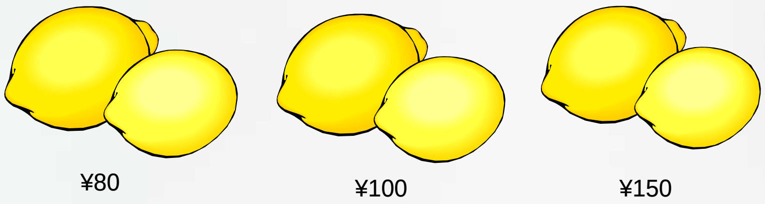


What’s wrong with squeezing more?

- IT budget is limited
  - Think about communication budget
- Developing countries can’t afford to deploy “secure version of IT”
- So does SME, SOHO, NPO, NGO...
- Then:
- What about selling inferior things for less?
- We don’t want price crunch in this market...

Market of lemons

- Fear for price crunch... Here’s why:



- How to tell “Good things for masses” from “Bad things for less”?
- Answer: clearinghouse.
- Suppose good things remain.
- How to crunch further?

Enter profile.

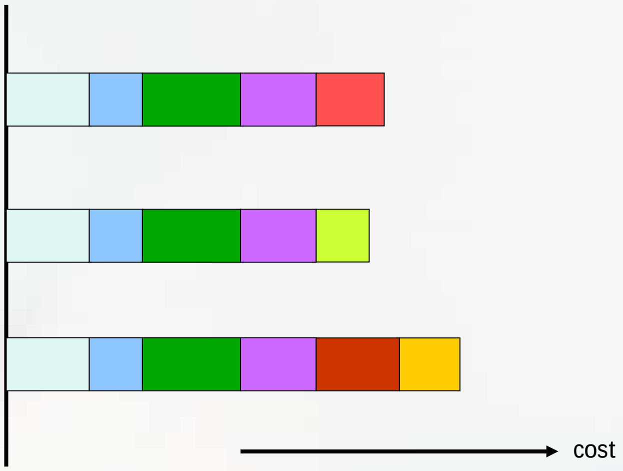
- Profile is here to improve cost efficiency
  - Design
  - Integration
  - Certification
  - Operation
- My definition of Profile:
  - A well-examined set of well-defined components
  - A certified “set of components”
  - A point beyond which further expert investigation is not necessary

Profile does exist

- The most successful profile to date:
  - HTTPS
  - The everyday vehicle of e-commerce
- Techie Quiz: do you know its RFC number?
- Then what is HTTPS?
  - It’s a Profile;
    a well-examined set of HTTP and SSL
  - Beyond which ISMS reviewers won’t investigate

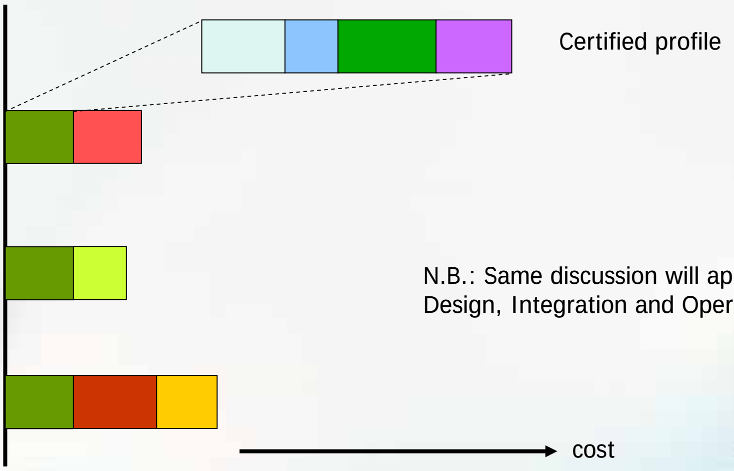
Cost structure of certification: 2004

- Without Profile, the certification cost skyrockets



Cost structure of certification: 2010

- With Profile, common set of components are certified once; certification costs are nominal

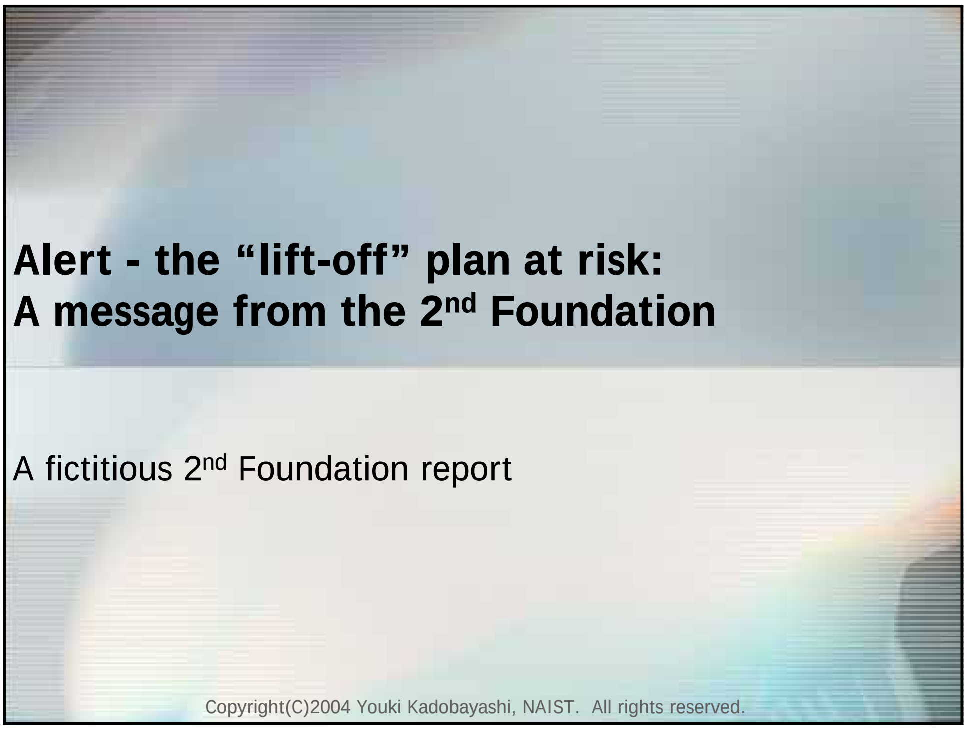


N.B.: Same discussion will apply to Design, Integration and Operation

Okay the future is bright!

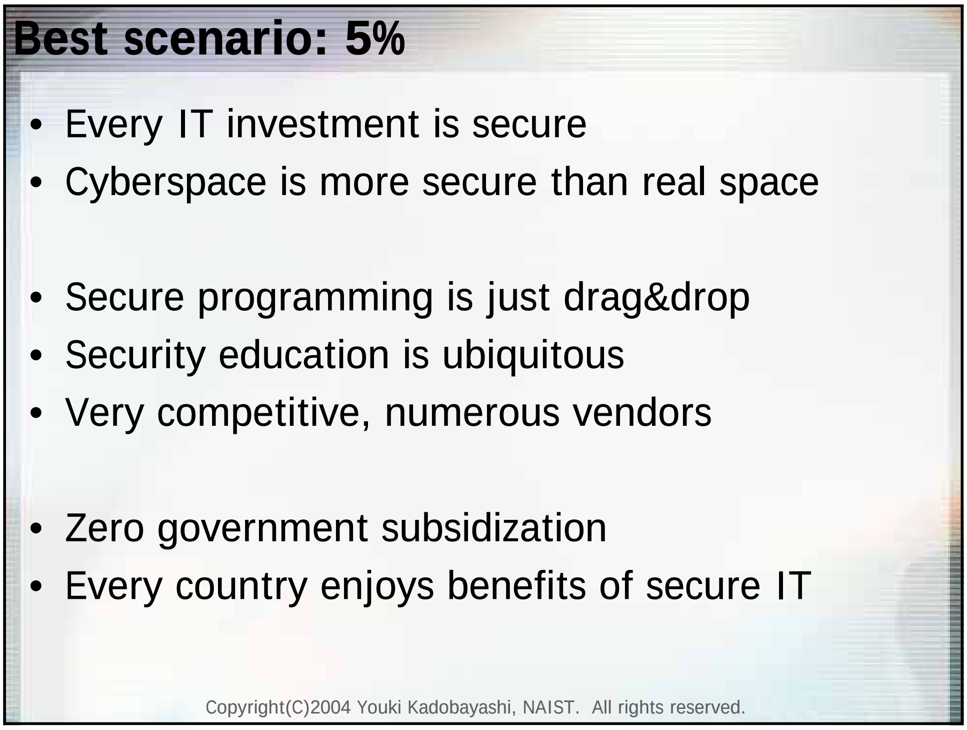
- I’ll develop profiles for banks!
- I’ll do it for logistics!
- I’ll do it for SOHO!
- I’ll do it for e-commerce shopping carts!

- Wait a minute, things are not that easy...



Alert - the “lift-off” plan at risk: A message from the 2nd Foundation

A fictitious 2nd Foundation report

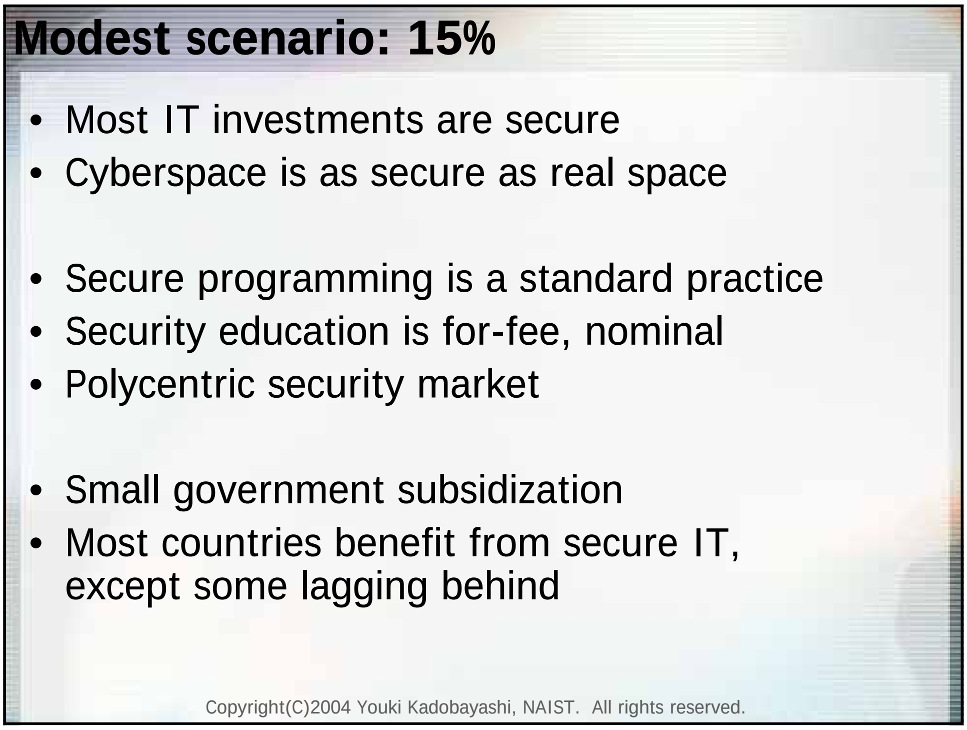


Best scenario: 5%

- Every IT investment is secure
- Cyberspace is more secure than real space

- Secure programming is just drag&drop
- Security education is ubiquitous
- Very competitive, numerous vendors

- Zero government subsidization
- Every country enjoys benefits of secure IT

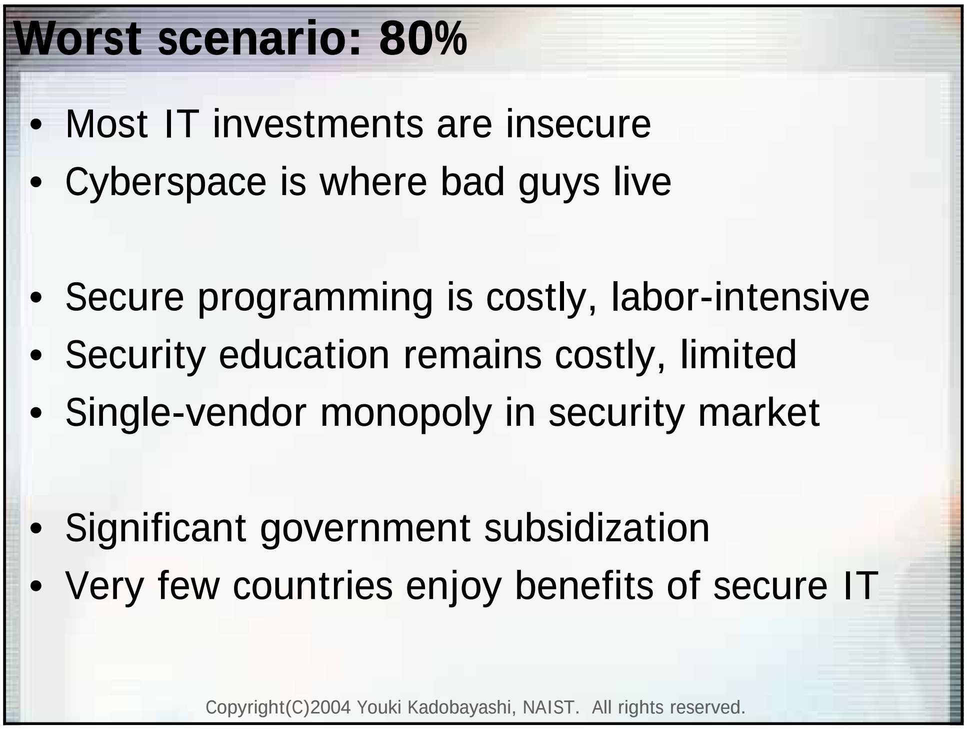


Modest scenario: 15%

- Most IT investments are secure
- Cyberspace is as secure as real space

- Secure programming is a standard practice
- Security education is for-fee, nominal
- Polycentric security market

- Small government subsidization
- Most countries benefit from secure IT, except some lagging behind

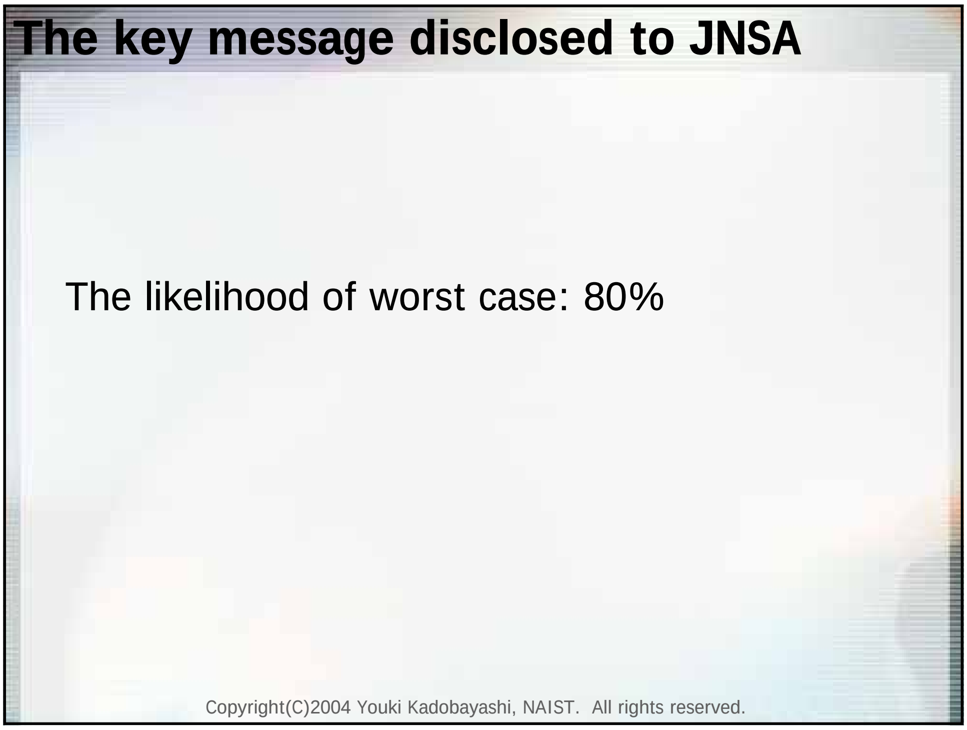


Worst scenario: 80%

- Most IT investments are insecure
- Cyberspace is where bad guys live

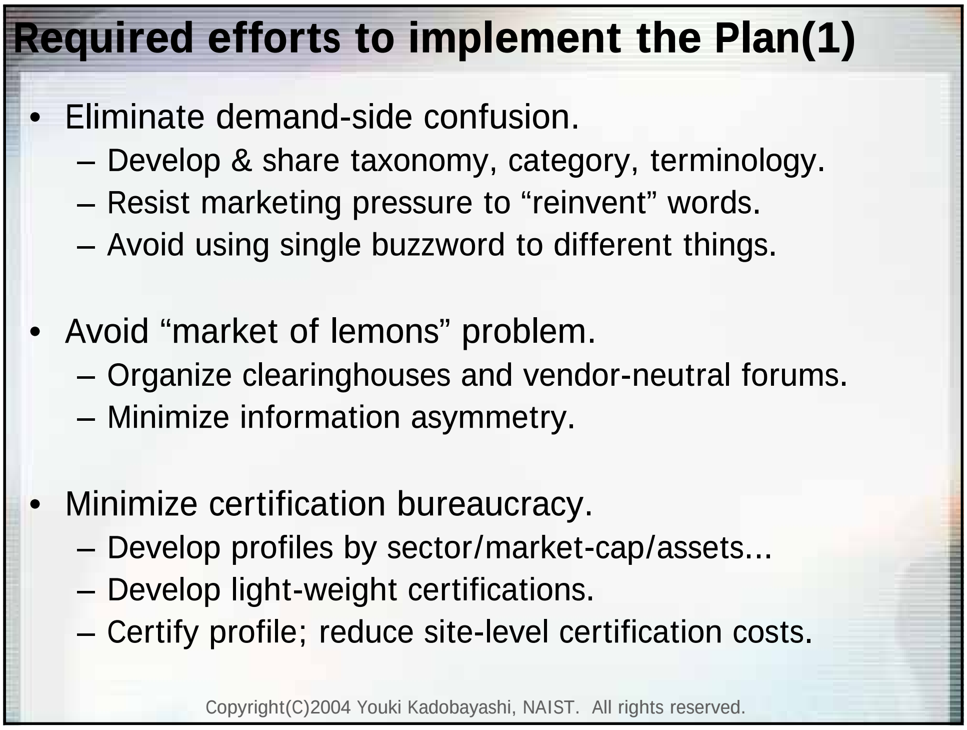
- Secure programming is costly, labor-intensive
- Security education remains costly, limited
- Single-vendor monopoly in security market

- Significant government subsidization
- Very few countries enjoy benefits of secure IT



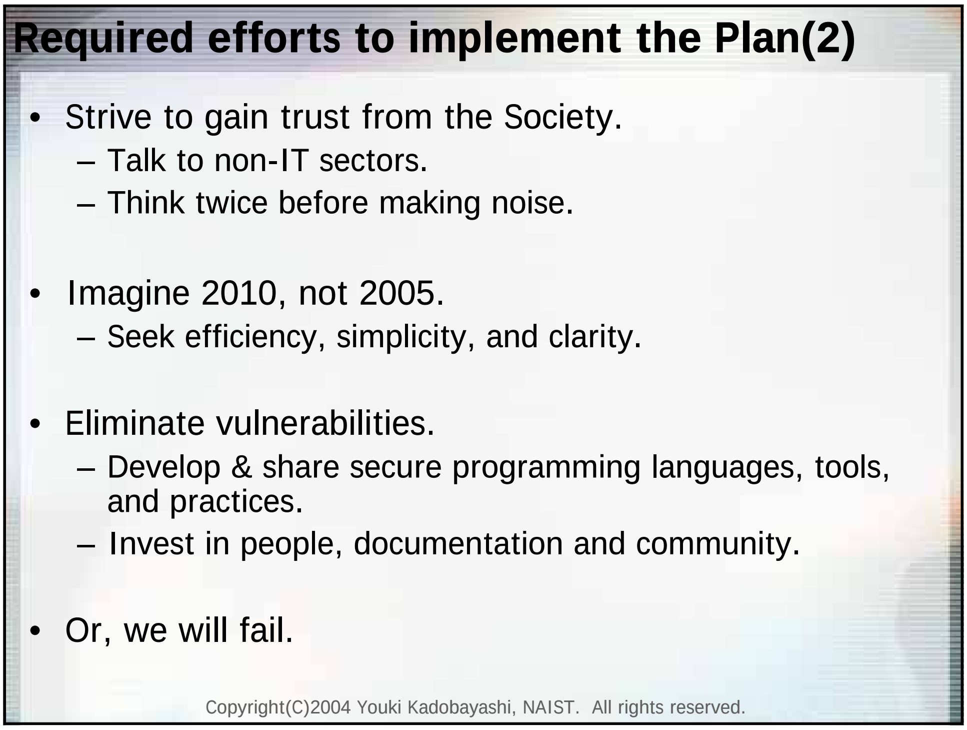
The key message disclosed to JNSA

The likelihood of worst case: 80%



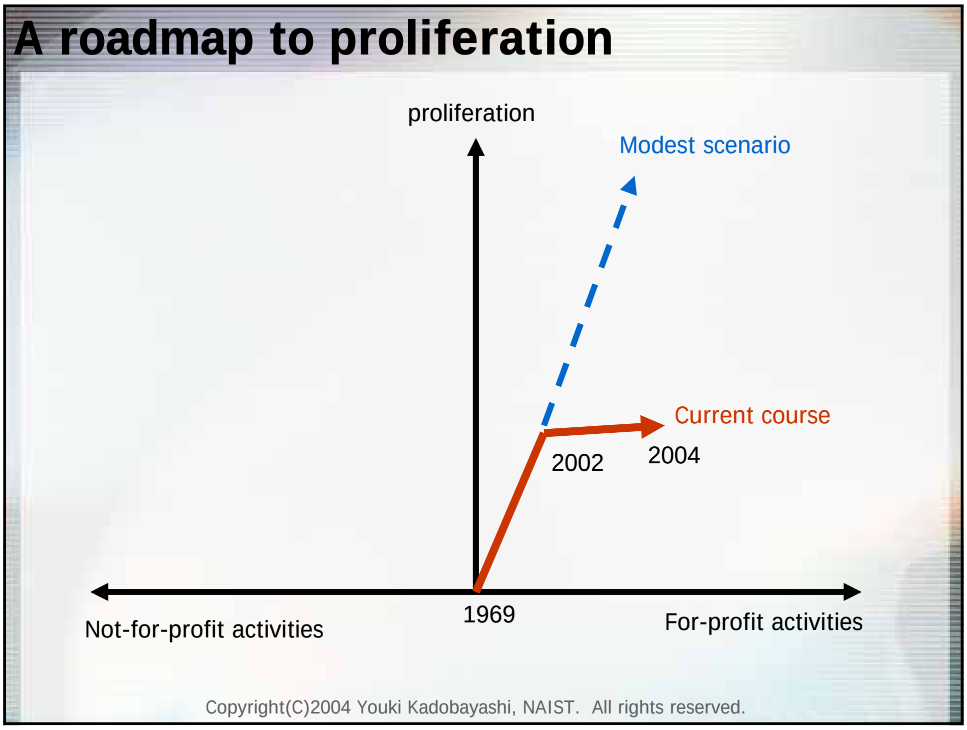
Required efforts to implement the Plan(1)

- Eliminate demand-side confusion.
  - Develop & share taxonomy, category, terminology.
  - Resist marketing pressure to “reinvent” words.
  - Avoid using single buzzword to different things.
- Avoid “market of lemons” problem.
  - Organize clearinghouses and vendor-neutral forums.
  - Minimize information asymmetry.
- Minimize certification bureaucracy.
  - Develop profiles by sector/market-cap/assets...
  - Develop light-weight certifications.
  - Certify profile; reduce site-level certification costs.



Required efforts to implement the Plan(2)

- Strive to gain trust from the Society.
  - Talk to non-IT sectors.
  - Think twice before making noise.
- Imagine 2010, not 2005.
  - Seek efficiency, simplicity, and clarity.
- Eliminate vulnerabilities.
  - Develop & share secure programming languages, tools, and practices.
  - Invest in people, documentation and community.
- Or, we will fail.



A roadmap to proliferation

proliferation

Modest scenario

Current course

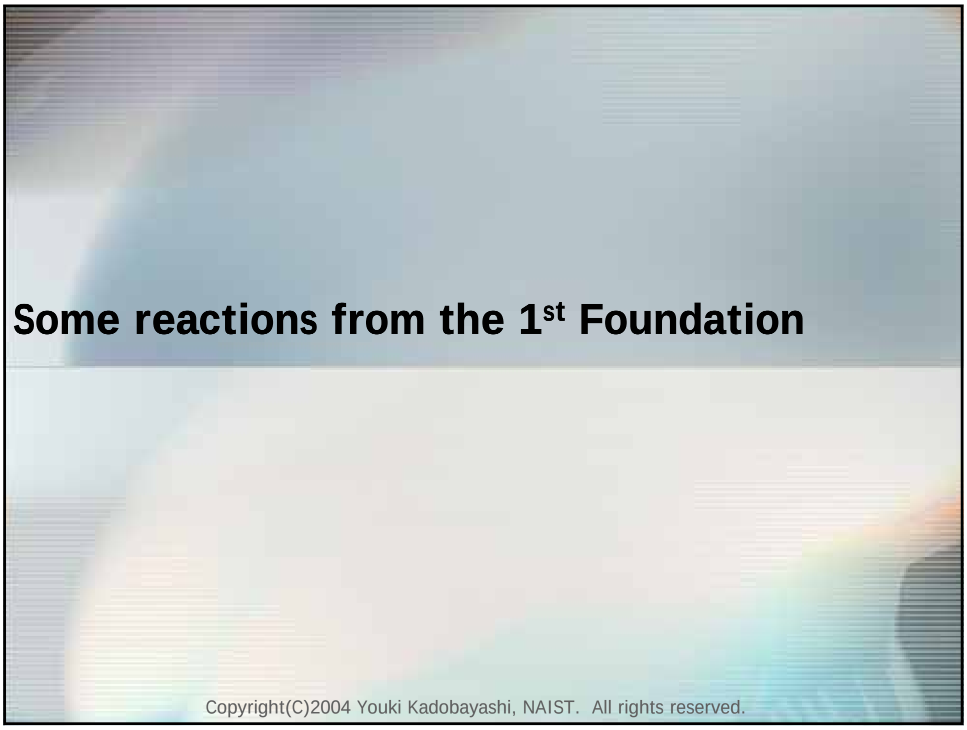
2002

2004

1969

Not-for-profit activities

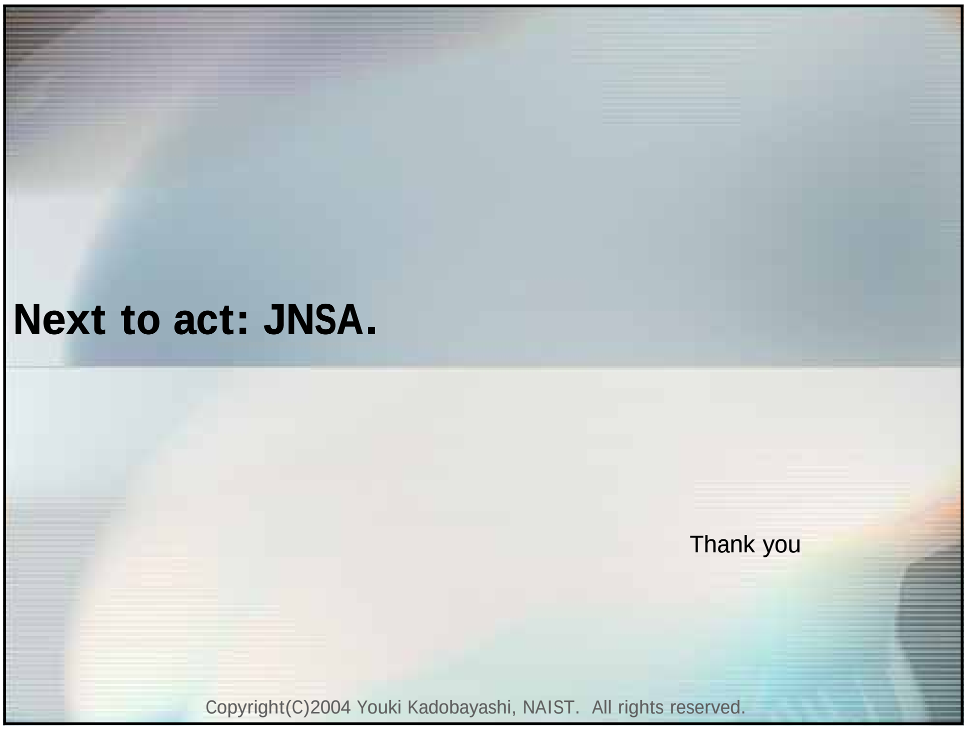
For-profit activities



Some reactions from the 1st Foundation

An approach in the…

- (to be presented at the conference)



Next to act: JNSA.

Thank you